Linear representations of braid groups and braid-based cryptography

Dissertation
zur Erlangung des Doktorgrades
der Naturwissenschaften
an der Fakultät für Mathematik
der Ruhr-Universität Bochum

vorgelegt von
Arkadius G. Kalka

9. Mai 2007

Dekan:	Prof. Dr. Holger Dette
1. Prüfer:	Prof. Dr. Lothar Gerritzen
2. Prüfer:	PD Dr. Ralf Holtkamp

Tag der mündlichen Prüfung: 6. Juli 2007

Prüfungskommission:

Prof. Dr. Gerhard Knieper (Vorsitzender)
Prof. Dr. Lothar Gerritzen
Prof. Dr. Christiane Helzel
PD Dr. Ralf Holtkamp
Prof. Dr. Werner Kirsch

Contents

Introduction

The aim of this work is the evaluation of braid-based cryptography by cryptanalysis and the introduction of new schemes.

Braid group cryptography, a relatively new branch of public key cryptography using feasible non-commutative groups, was introduced in [**AAG99**] and [**KL$^+$00**]. A motivation and a very short review of the history of non-commutative cryptography, of which braid group cryptography is a branch, is given at the beginning of chapter 5. Section 5.1 describes the fundamental braid-based key agreement protocols [**AAG99**, **KL$^+$00**, **CK$^+$01**] for general groups and their base problems. In section 5.2 we discuss several attacks against the above mentioned key agreement protocols which were proposed so far.

The AAG [**AAG99**] and the Ko-Lee et al. scheme [**KL$^+$00**] were early compromised by Gebhardt's practically efficient solution to the conjugacy search problem in braid groups for randomly chosen, long input braids [**Ge05**]. Therefore we focussed our cryptanalytical efforts to the braid Diffie-Hellman KAP (section 4.1) [**CK$^+$01**], a revised Ko-Lee protocol, based on a decomposition problem in braid groups. As cryptanalytical tool we used representation attacks. The idea is, using linear representations of the braid group B_n, to solve the base problem in a matrix group, and then lift back to B_n. We improved the two known representation attacks on the braid Diffie-Helman KAP [**CK$^+$01**], the Lee-Park attack (section 4.2.2) [**LP03**] using Burau representation, and the Cheon-Jun attack (section 4.2.1) [**CJ03a**, **CJ03b**] using Lawrence-Krammer representation.

After a short review of several notions and fundamental properties of braid groups in section 1.1 we introduce the fundamental representations in question, the Burau representation $\beta : B_n \to GL(n, \mathbb{Z}[q^{\pm 1}])$ (section 1.2) and the Lawrence-Krammer representation $\rho : B_n \to GL(\binom{n}{2}, \mathbb{Z}[q^{\pm 1}, t^{\pm 1}])$ (section 1.3) [**La90**]. In section 1.4 we show that the Lawrence-Krammer module for $t = 1$ is isomorphic to the symmetric square of the reduced Burau module [**Kr00**]. But there is a further connection between the Burau and the Lawrence-Krammer representation: There exists an iterated construction of

braid representations, called augmenting construction, which generalizes the construction of Magnus representations. The augmenting construction (section 1.5), independently introduced in [**BLM92**] and [**L92**], yields, starting with the trivial representation, the Burau representation. And if we apply it to the Burau representation, we get an n^2-dimensional representation which can be reduced to the Lawrence-Krammer representation [**Lo94**].
Since the Lawrence-Krammer representation is proved to be faithful for all $n \in \mathbb{N}$ [**Bi00**, **Kr02**] we are able to compute the unique preimage braid of a given Lawrence-Krammer matrix. Chapter 2 deals with inversion algorithms for the Lawrence-Krammer representation. Indeed, there is a deep connection between the Lawrence-Krammer representation and efficiently computable normal forms of the braid group, the Garside or greedy normal forms. All Garside groups admit such greedy normal forms. The notion of Garside monoids and groups is introduced in section 2.1. Note that there are two (known) Garside monoids in B_n, the monoid of positive braids B_n^+ in the classical Artin presentation, and the dual monoid BKL_n^+, consisting of those braids which are positive according to the dual (or Birman-Ko-Lee) presentation. Indeed, we are able to reconstruct the unique preimage braid of a given Lawrence-Krammer matrix directly in greedy and dual greedy normal form. In order to explain why a reconstruction in greedy normal form is always possible we review in section 2.2 the main steps of Krammer's combinatorial faithfulness proof for the Lawrence-Krammer representation setting $q \in (0,1)$ [**Kr02**]. Further, Krammer's faithfulness proof for the Lawrence-Krammer representation of B_4 with $t \in (0,1)$ [**Kr00**] is reviewed in detail in section 2.3. Indeed, we present a slightly different, quite longer proof, which has the advantage that the definition of the cones C_y (see proof of Theorem 2.38) is more unified. This faithfulness proof of $\rho_4|_{t\in(0,1)}$ leads to an inversion algorithm (which is an inversion heuristic for $n \geq 5$ with 100% success rate) that reconstructs the preimage braid in dual Garside normal form. Both inversion algorithms for the Lawrence-Krammer representation are explicitly given in section 2.4.
Contrary to the Lawrence-Krammer representation, the Burau representation is not faithful for $n \geq 5$ [**Bi99**]. Since the structure of the Burau kernel is not understood so far, only heuristics for the computation of preimage braids are known. In the sections 3.1 and 3.2 we describe Hughes' algorithm [**Hu02**] and its improvements by E. Lee and Park [**LP03**]. In section 3.3 we first construct an inversion heuristic (with 100% success rate) for the above mentioned n^2-dimensional representation arising from augmenting construction. Then we apply an analgue of this heuristic to the Burau representation. This yields a linear time inversion heuristic for the Burau representation (algorithm 3.5) with sligthly, but significantly better success rates than the

linear time heuristics described in section 3.1. Of course, algorithm 3.5 provides an improved Lee-Park attack against the braid Diffie-Hellman KAP (section 4.2.2).
Further, using ideas from [**LP03**], we improved Cheon-Jun attack using Lawrence-Krammer representation. Though our attack (section 4.3) is not deterministic, for generic, sufficiently long instance braids, we can recover the ρ-image of the private key using only one matrix inversion. This result was already published in [**Ka06**]. A complexity analysis (section 4.3.3) shows that our attack is 3τ orders in n more efficient than Cheon-Jun attack, where τ denotes the matrix multiplication exponent.
Nevertheless, a completely different and more efficient heuristic attack had been proposed by Myasnikov, Shpilrain and Ushakov at the CRYPTO 2005 [**MSU05**]. We describe this attack in section 5.2.4. Further, Shpilrain and Ushakov introduced a new key agreement protocol based on a generalized decomposition problem (section 5.3) [**SU06b**].
KAPs are not the only braid-based cryptographic primitives. In section 5.4 we deal with signature and authentication schemes. Special attention deserves the Fiat-Shamir-like authentication scheme using shifted conjugacy (section 6.2), introduced by P. Dehornoy [**De06**]. Shifted conjugacy is a (left) self-distributive binary operation in the infinite braid group $B_{\mathbb{N}}$. Together with other examples for LD-systems it is discussed in section 6.1. The base problem of Dehornoy's authentication scheme [**De06**] is the shifted conjugacy search problem, for which, contrary to the usual conjugacy search problem in braid groups, no solution is known so far.
We tried to invent a new key agreement protocol based on shifted conjugacy in braid groups. It turned out that we are able to adapt the AAG scheme. We show in section 6.3 that the AAG protocol for monoids naturally generalizes to an AAG protocol for magmas. Further, we show that the most natural special case of this general scheme is a key agreement scheme for LD-systems. In section 6.4 we construct an explicit KAP, which is based on a simultaneous shifted conjugacy search problem in braid groups. As a further example of the general AAG scheme for magmas we introduce in section 6.3.2 a KAP based on a simultaneous decomposition problem in groups.
We believe that the above mentioned variants of the AAG protocol are not the only specifications of our general AAG scheme for magmas and that it should provide plenty more concrete examples. In particular Laver tables seem to provide other interesting platform LD systems. But this is dedicated to future work.
We note that the ideas introduced in section 6.3 inspired us to repair a further Fiat-Shamir-like authentication scheme for LD-systems (section 6.2), introduced by P. Dehornoy in a talk given at a workshop in Bochum [**De05**].

Acknowledgements

I wish to thank my supervisor L. Gerritzen for his kind support, encouragement, constant interest and steadfast patience. In particular I thank him that I could take part in the organization of the international workshop "Algebraic Methods in Cryptography" (17.-18.11.2005) at the Ruhr-Universität Bochum. For valuable hints or stimulating discussions I thank R. Avanzi, P. Dehornoy, M. Kreuzer, E. Lee, S. J. Lee, M. Paterson, A. Razborov, G. Rosenberger, V. Shpilrain, B. Tsaban and A. Ushakov. In particular I wish to thank B. Tsaban for his efforts concerning the CGC Bulletin, dedicated to combinatorial group theory and cryptography. My thanks also go to all the nice people I have met at the "Lehrstuhl für Algebra and Geometrie". In particular I thank R. Holtkamp for refereeing my thesis.
Further, I would like to acknowledge financial support by the Graduate College "Mathematische und ingenieurwissenschaftliche Methoden für sichere Datenübertragung und Informationsvermittlung" (speaker: G. Frey). Here I wish to thank H. Flenner, L. Gerritzen and U. Storch who encouraged and helped me to apply for this grant.
Finally, I wish to thank my father for his lovable support over many years.

Chapter 1

On some linear representations of braid groups

1.1 Braid groups: several notions and fundamental properties

This section deals with the definition and fundamental properties of the braid groups, which were introduced by E. Artin in 1926 [**Ar26**, **Ar47**]. For more details on braids and braid groups we refer to [**Bi74**, **MK99**, **BB06**]. Several of our notations are used as in [**Bi74**].

Definition 1.1 *Consider the so-called* big diagonal *in* $\mathbb{C}^n$,

$$\Delta := \{(z_1, \ldots, z_n) \in \mathbb{C}^n \mid z_i = z_j \quad \text{for some} \quad i \neq j\}.$$

Choose a fixed base point z^0 *in* $\mathbb{C}^n \backslash \Delta$*, e.g., defined by* $z^0 = (z_1^0, \ldots, z_n^0) = (1, \ldots, n)$*. Then the fundamental group* $P_n := \pi_1(\mathbb{C}^n \backslash \Delta, z^0)$ *is called the* pure *(or* unpermuted *or* colored*)* braid group (with n strands)*.*

There exists a natural left[1] action of the symmetric group $S_n = (S_n, \circ)$ on $\mathbb{C}^n \backslash \Delta$, permuting the coordinates in $z \in \mathbb{C}^n \backslash \Delta$:

$$\begin{array}{rcl} S_n \times \mathbb{C}^n \backslash \Delta & \longrightarrow & \mathbb{C}^n \backslash \Delta \quad \text{defined by} \\ (\sigma, (z_1, \ldots, z_n)) & \longmapsto & (z_{\sigma(1)}, \ldots, z_{\sigma(n)}). \end{array}$$

The orbit space $(\mathbb{C}^n \backslash \Delta)/S_n$ is called configuration space, and the orbit space projection $p : \mathbb{C}^n \backslash \Delta \to (\mathbb{C}^n \backslash \Delta)/S_n$ is a regular covering projection.

[1] We use the notation $(\sigma \circ \tau)(i) := \sigma(\tau(i))$.

Definition 1.1 (continued)
The fundamental group of the configuration space, $B_n := \pi_1((\mathbb{C}^n \backslash \Delta)/S_n)$, is (called) the (full) braid group (with n strands)*. The elements of P_n and B_n are called* pure braids *and* braids*, respectively. The neutral element of P_n and B_n is called* trivial braid *and denoted by e or 1.*

A braid is represented by a loop $f : [0,1] \longrightarrow (\mathbb{C}^n \backslash \Delta)/S_n$, i.e., $f(0) = f(1) = p(z^0)$. This loop lifts uniquely to a path

$$\hat{f} = (\hat{f}_1, \ldots, \hat{f}_n) : [0,1] \to \mathbb{C}^n \backslash \Delta \quad \text{with} \quad \hat{f}(1) = z^0.$$

The graph $s_i := \{(\hat{f}_i(t), t) \in \mathbb{C} \times [0,1] \mid t \in [0,1]\}$ of the i-th coordinate function $\hat{f}_i : [0,1] \to \mathbb{C}$ can be viewed as the i-th braid strand and the union $s := s_1 \cup \ldots \cup s_n$ as a geometric braid.
This unique lift $\hat{f}$ of f allows us to define the surjective homomorphism

$$\begin{array}{rcll} \nu : B_n = \pi_1((\mathbb{C}^n \backslash \Delta)/S_n) & \longrightarrow & S_n & \text{by} \\ f & \longmapsto & \left(\begin{array}{c} \hat{f}_1(1), \ldots, \hat{f}_n(1) \\ \hat{f}_1(0), \ldots, \hat{f}_n(0) \end{array} \right). & \end{array}$$

Here we define the braid permutation or induced permutation $\nu(f)$ by specifying the initial positions $\hat{f}_i(0)$ in terms of the final positions $\hat{f}_i(1)$ $\forall i = 1, \ldots, n$. Otherwise we would get an anti-homomorphism instead of a homomorphism. Together with the injective homomorphism p_* induced by the covering projection p, this surjective homomorphism ν gives rise to a short exact sequence

$$1 \longrightarrow P_n \xrightarrow{p_*} B_n \xrightarrow{\nu} S_n \longrightarrow 1$$

with im $p_* = \ker \nu = P_n$. This short exact sequence is not split, since there exists no monomorphism from S_n to B_n. And this is true, because the braid group is torsion free, i.e., there exists no $b \in B_n$ such that $b^k = e$ for some $k \geq 1$. An older proof for the fact that B_n contains no elements of finite order is given in [**Mu82**]. See also the proof to Proposition 10.14 in [**BZ03**], using Satz 4.1 of [**Wa67**]. Dehornoy's fundamental discovery of a left-invariant total order[2] $<$ on B_n [**De94**, **De00**] yields a very short proof (see also section 6.4 in [**BB06**]):
Let $b \neq e$ be a braid with $e < b$. Now, left-invariance of the order $<$ implies

$$\ldots < b^{-3} < b^{-2} < b^{-1} < e < b < b^2 < b^3 < \ldots .$$

Further, replace in the case $e > b$ "$<$" by "$>$" which proves the assertion.

[2] A group G admits a left-invariant order $<$ if $b < c \Rightarrow ab < ac$ $\forall a, b, c \in G$.

Now, since P_n is a subgroup of index $n!$ in B_n, it turns out to be sufficient for our purposes to consider presentations of B_n:

Proposition 1.2 *Denote* $\mathrm{i} = \sqrt{-1} \in \mathbb{C}$. *For all* $k = 1, \ldots, n-1$, *let the* k-th Artin generator[3] $\sigma_k \in B_n$ *be represented, e.g., by the path*

$$\begin{array}{rcl} [0,1] & \longrightarrow & \mathbb{C}^n \backslash \Delta, \\ t & \longmapsto & (1, \ldots, k-1, k+t-\mathrm{i}\sqrt{t-t^2}, k+1-t+\mathrm{i}\sqrt{t-t^2}, \ldots, n), \end{array}$$

then B_n *admits the well-known* Artin presentation

$$B_n = \left\langle \sigma_1, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & \forall |i-j| > 1, \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} & \forall i = 1, \ldots, n-2 \end{array} \right\rangle.$$

Proof. - See, e.g., [**Ar47**] or theorem 1.8 in [**Bi74**]. □

A new presentation with an enlarged set of generators (so-called band generators[4])

$$\begin{array}{rcl} a_{ts} & = & (\sigma_{t-1} \cdots \sigma_{s+1})\sigma_s(\sigma_{s+1}^{-1} \cdots \sigma_{t-1}^{-1}) \\ & = & (\sigma_s^{-1} \cdots \sigma_{t-2}^{-1})\sigma_{t-1}(\sigma_{t-2} \cdots \sigma_s), \quad 1 \le s < t \le n, \end{array}$$

and relations

$$\begin{array}{rl} a_{ts}a_{sr} = a_{sr}a_{tr} = a_{tr}a_{ts}, & 1 \le r < s < t \le n, \\ a_{ts}a_{rq} = a_{rq}a_{ts}, & (t-r)(t-q)(s-r)(s-q), \end{array}$$

was introduced in [**Xu92**, **Br94**, **KKL97**, **BKL98**]. We call this presentation BKL- or dual presentation.

Further, we can view B_n as the mapping class group of the n-punctured disc:

Definition 1.3 (see [**Kr00**]) *Let* $D = D^{(n)} := \{z \in \mathbb{C} \mid |z - \frac{1}{2}(n+1)| \le \frac{1}{2}(n+1)\}$ *be the disc in* $\mathbb{C}$ *with diameter* $[0, n+1]$, *and denote the correpond-ing* n-punctured disc *by* $D_n := D \backslash \mathcal{P}$ *with* $\mathcal{P} := \{z_1^0, \ldots, z_n^0\} = \{1, \ldots, n\}$. *Let* $H = H(D, \mathcal{P})$ *be the group of all orientation-preserving homeomorphisms* $\phi : D \to D$ *satisfying* $\phi\mid_{\partial D} = \mathrm{id}$ *and* $\phi(\mathcal{P}) = \mathcal{P}$. *The group structure on* H

[3] Informally speaking, inside the Artin generator σ_k the $(k+1)$-th strand crosses over the k-th strand, and vice versa for the inverse generator σ_k^{-1}.

[4] Loosely speaking, inside the band generator a_{ts} the t-th strand crosses over the s-th strand in front of the strands $s+1, \ldots, t-1$.

is simply given by composition.
By H_0 we denote the (normal) subgroup of H, consisting of those $\phi \in H$ which are isotopic to the identity element, i.e., there exists a continous isotopy $I : [0,1] \times D \to D$ such that $I(0,z) = z$, $I(1,z) = \phi(z)$ $\forall z \in D$ and $(I(t,\cdot) : D \to D) \in H$ for all $t \in [0,1]$.
Then we can define the mapping class group of D_n, *i.e. the* mapping class group of D relative to $\mathcal{P}$, *as the group of orientation-preserving self-homeomorphisms of D which keep the boundary ∂D pointwise and $\mathcal{P}$ as a set fixed:*

$$\mathcal{M}(D_n) = \mathcal{M}(D, \mathcal{P}) := H/H_0.$$

Definition 1.4 *Let γ be an embedded arc in D_n whose endpoints are punctures. A* Dehn half twist *is a homeomorphism $\tau_\gamma \in \mathcal{M}(D_n)$ which is the identity map outside a regular neighbourhood of γ and which exchanges the endpoint punctures. Identifying this arc with a straight line, the homeomorphism τ_γ is obtained by rotating γ about its midpoint to the angle of π in counterclockwise direction.*

Proposition 1.5 *The mapping $B_n \to \mathcal{M}(D_n)$ defined by $\sigma_k \mapsto \tau_{[k,k+1]}$ $(1 \leq k < n)$ is a group isomorphism.*

Proof. - A proof is sketched in section 1.1.2 of [**DD$^+$02**]. For details we refer to chapter 4 in [**Bi74**] or section 1.3 in [**BB06**].

An orientation-preserving homeomorphism $\phi : D \to D$ with $\phi(\mathcal{P}) = \mathcal{P}$ which keeps the boundary ∂D pointwise fixed can be recovered up to isotopy from the induced isomorphism $\phi_* : \pi_1(D_n, z_*) \to \pi_1(D_n, z_*)$, where $z_* \in \partial D$ is a fixed base point. This gives rise to an embedding

$$\imath : B_n \cong \mathcal{M}(D_n) \longrightarrow \mathrm{Aut}(\pi_1(D_n, z_*)) = \mathrm{Aut}(F_n).$$

If we choose $z_* = n+1$ and $\{x_i \mid i = 1, \ldots, n\}$ (Figure 1.1) as generator set of $F_n \cong \pi_1(D_n, z_*)$, then the monomorphic image of an Artin generator is $\forall k = 1, \ldots, n-1$:

$$\begin{array}{rcl} \imath(\sigma_k) : F_n & \longrightarrow & F_n, \\ x_i & \longmapsto & \begin{cases} x_{k+1}, & i = k, \\ x_{k+1}^{-1} x_k x_{k+1}, & i = k+1, \\ x_i, & i \neq k, k+1. \end{cases} \end{array}$$

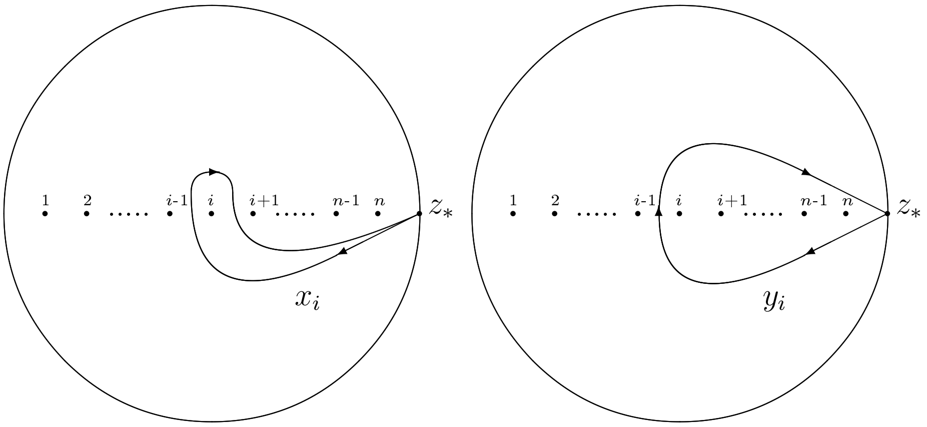


Figure 1.1: Paths representing the Generators x_i and y_i of $\pi_1(D_n, z_*)$.

In the case $F_n \cong \pi_1(D_n, z_*) = \langle y_1, \ldots, y_n \rangle$ (Figure 1.1) we get $\forall k = 1, \ldots, n-2$:

$$\begin{array}{rcl} \imath(\sigma_k) : F_n & \longrightarrow & F_n, \\ y_i & \longmapsto & \left\{ \begin{array}{ll} y_{k+2} y_{k+1}^{-1} y_k, & i = k+1 \\ y_i, & i \neq k+1 \end{array} \right. \quad \text{and} \\ \imath(\sigma_{n-1}) : F_n & \longrightarrow & F_n, \\ y_i & \longmapsto & \left\{ \begin{array}{ll} y_n^{-1} y_{n-1}, & i = n \\ y_i, & i \neq n. \end{array} \right. \end{array}$$

Note the following relations between the x_i's and the y_i's:

$$x_i = y_i y_{i+1}^{-1}, \quad y_i = x_i x_{i+1} \cdots x_n \quad \forall 1 \leq i < n, \quad \text{and} \quad x_n = y_n.$$

Proposition 1.6 *There exists a natural embedding*

$$\begin{array}{rcl} \alpha : F_n & \longrightarrow & P_{n+1} \quad \textit{defined by} \\ x_i & \longmapsto & \left\{ \begin{array}{lll} \hat{f} : & [0,1] & \longrightarrow \mathbb{C}^n \backslash \Delta \\ & t & \longmapsto (1, \ldots, n, x_i(t)) \end{array} \right. \end{array}$$

such that the subgroup of P_{n+1} generated by $\alpha(x_1), \ldots, \alpha(x_n)$ is a free group. Further this free subgroup is normal in P_{n+1}, but it is not a normal subgroup of B_{n+1}.

Proof. - See, e.g., chapter 3.2 in [**MK99**].

Embed $\mathbb{C} \times [0,1]$ in the 3-dimensional space such that the real and imaginary axes lie in $(1,0,0)^T$- and $(0,1,0)^T$-direction, respectively, and the t-axis lies in $(0,0,-1)^T$-direction. Now, if we view along the imaginary axis, then we see that $\hat{f} : t \mapsto (1, \ldots, n, x_i(t))$ describes the pure braid $A_{i,n+1} := a^2_{n+1,i} \in P_{n+1}$. The A_{ij}'s $(1 \leq i < j \leq n)$ build a classical generating set of the pure braid group P_n, introduced by E. Artin. Further, if we define $B_{ij} = A_{ij} A_{i+1,j} \cdots A_{j-1,j}$, then $\alpha(x_i) = A_{i,n+1}$ implies $\alpha(y_i) = B_{i,n+1}$. It is easy to verify that the following braid identities hold in B_{n+1}:

$$\sigma_k A^{\pm 1}_{k,n+1} \sigma_k^{-1} = A^{\pm 1}_{k+1,n+1}, \quad \sigma_k A^{\pm 1}_{k+1,n+1} \sigma_k^{-1} = A^{-1}_{k+1,n+1} A^{\pm 1}_{k,n+1} A_{k+1,n+1},$$

and $\sigma_k A^{\pm 1}_{j,n+1} \sigma_k^{-1} = A^{\pm 1}_{j,n+1}$ for all $j \neq k, k+1$. This implies

$$\sigma_k \alpha(x_j^{\pm 1}) \sigma_k^{-1} = \alpha(\imath(\sigma_k)(x_j^{\pm 1})) \quad \text{for all} \quad 1 \leq j \leq n, \ 1 \leq k < n.$$

Analogously we verify $\sigma_k^{-1} \alpha(x_j^{\pm 1}) \sigma_k = \alpha(\imath(\sigma_k^{-1})(x_j^{\pm 1}))$. Now, we can simply prove by induction that

$$b \alpha(w) b^{-1} = \alpha(\imath(b)(w)) \quad \forall b \in B_n, \ \forall w \in F_n.$$

Therefore, if we do not distinguish between $w \in F_n$ and $\alpha(w) \in P_{n+1}$, then we can say that B_n acts from left on F_n by conjugation.

Together with the surjective homomorphism $\xi : P_{n+1} \to P_n$ defined by pulling out the $(n+1)$-th strand, the embedding α gives rise to the short exact sequence

$$1 \longrightarrow F_n \xrightarrow{\alpha} P_{n+1} \xrightarrow{\xi} P_n \longrightarrow 1.$$

Because of the (injective) homomorphism $\jmath : P_n \to P_{n+1}$ with $\xi \circ \jmath = \mathrm{id}_{P_n}$, this short exact sequence is split, i.e., $P_{n+1} = F_n \rtimes P_n$. By induction P_n becomes an iterated semidirect product of free subgroups:

$$P_n = F_{n-1} \rtimes (F_{n-2} \rtimes (F_{n-3} \rtimes \ldots (F_2 \rtimes F_1))).$$

This yields the so-called combed normal form of pure braids. Since every braid b can be written as product of a pure braid and a permutation braid[5] with induced permutation $\nu(b)$, this also provides a solution to the word-problem in B_n.

But the Artin combing algorithm [**Ar47**, **Bi74**] works quite slowly. It seems

[5] A permutation braid is a positive braid where every pair of strands crosses at most once. Consider the set $\{\tau_i = (i, i+1) \mid i = 1, \ldots, n-1\}$ of nearest neighbour transpositions, which is a generating set of S_n. Now, a permutation braid $b_\sigma \in B_n$ can be obtained from its induced permutation $\sigma \in S_n$ in the following way: Choose a positive word w in the τ_i's with minimal length representing the permutation σ. Then replace each τ_i by a σ_i.

to have a time complexity which is exponential in the wordlength of a given instance braid word. Nevertheless, no complexity bounds seem to have been proven so far. An example for a braid, represented by a relatively short braid word, for which the combing algorithm takes a quite long time, is given by the Burau kernel element of B_5, discovered by S. Bigelow [**Bi99**].

1.2 Burau representation

A linear representation of the braid group B_n is a homomorphism $B_n \to GL(k, R)$ for some $k \in \mathbb{N}$ and a ring R.
The Burau representation

$$\begin{array}{rcl} \beta : B_n & \longrightarrow & GL(n, \mathbb{Z}[q^{\pm 1}]) \quad \text{defined by} \\ \sigma_i & \longmapsto & \mathrm{Id}_{i-1} \oplus \begin{pmatrix} 1-q & q \\ 1 & 0 \end{pmatrix} \oplus \mathrm{Id}_{n-i-1} \end{array}$$

was the first non-trivial representation of B_n, introduced in 1935 [**Bu36**]. It can be viewed as a deformation of the standard representation of S_n, i.e., substituting $q = 1$ gives back the representation of B_n which factors through S_n. Like the standard representation of S_n, which is known to be reducible, the Burau representation β splits into an $(n-1)$-dimensional irreducible representation, the reduced Burau representation

$$\begin{array}{rcl} \beta_{\text{red}} : B_n & \longrightarrow & GL(n-1, \mathbb{Z}[q^{\pm 1}]) \quad \text{defined by} \\ \sigma_1 & \longmapsto & \begin{pmatrix} -q & 1 \\ 0 & 1 \end{pmatrix} \oplus \mathrm{Id}_{n-i-3}, \\ \sigma_i & \longmapsto & \mathrm{Id}_{i-2} \oplus \begin{pmatrix} 1 & 0 & 0 \\ q & -q & 1 \\ 0 & 0 & 1 \end{pmatrix} \oplus \mathrm{Id}_{n-i-2} \quad , i = 2, \ldots, n-2, \\ \sigma_{n-1} & \longmapsto & \mathrm{Id}_{n-3} \oplus \begin{pmatrix} 1 & 0 \\ q & -q \end{pmatrix}, \end{array}$$

and the trivial 1-dimensional representation.

The Burau representation can be introduced as a Magnus representation[6] using Fox's free diffrential calculus [**Fo53**]. Another derivative of the Burau

[6] For an introduction in the theory of Magnus representations, see chapter 3 in [**Bi74**] or [**Ma74**]. The first such representation was probably introduced in 1939 by W. Magnus [**Ma39**].

representation is given in [**Lo89**]. But here we present a homological interpretation of the reduced Burau representation (see, e.g. [**Bi99**]):
Consider the homomorphism

$$\begin{array}{rcll}\Phi : \pi_1(D_n, z_*) = \langle x_1, \dots, x_n\rangle & \longrightarrow & \langle q\rangle \cong \mathbb{Z} & \text{defined by}\\ x_i & \longmapsto & q. & \end{array}$$

Let $\tilde{D}_n$ be the covering space corresponding to the subgroup $\ker\Phi$ of $\pi_1(D_n, z_*)$, i.e., $\gamma \in \pi_1(D_n, z_*)$ is lifted to a closed path in $\tilde{D}_n$ if and only if $\gamma \in \ker\Phi$. A concrete description of $\tilde{D}_n$ is given in [**Bi02**].
Let $\tilde{z}_*$ be a fixed point in the fibre $p^{-1}(z_*)$, where p denotes the covering projection from $\tilde{D}_n$ onto D_n. Then a braid, thought as an element $\phi \in \mathcal{M}(D_n)$, induces a unique lift $\tilde{\phi}$ with $\tilde{\phi}(\tilde{z}_*) = \tilde{z}_*$, i.e., $\tilde{\phi}$ makes the following diagram commute:

$$\begin{tikzcd}(\tilde{D}_n, \tilde{z}_*) \arrow[r, "\tilde{\phi}"] \arrow[d, "p"'] & (\tilde{D}_n, \tilde{z}_*) \arrow[d, "p"] \\ (D_n, z_*) \arrow[r, "\phi"'] & (D_n, z_*)\end{tikzcd}$$

The group of covering transformations of $\tilde{D}_n$ is $\mathrm{Cov}(\tilde{D}_n/D_n) = \langle q\rangle \cong \mathbb{Z}$. So, multiplicating a cycle $\tilde{\gamma} \in H_1(\tilde{D}_n)$ by q can be considered as the induced action of the covering transformation q. In so far $H_1(\tilde{D}_n)$ gets a $\mathbb{Z}[q^{\pm 1}]$-module structure. We call $H_1(\tilde{D}_n)$ the reduced Burau module.
The reduced Burau representation is the homomorphism

$$\begin{array}{rcl}\beta_{\text{red}} : B_n \cong \mathcal{M}(D_n) & \longrightarrow & \mathrm{Aut}(H_1(\tilde{D}_n)),\\ \phi & \longmapsto & \tilde{\phi}_*,\end{array}$$

where $\tilde{\phi}_* : H_1(\tilde{D}_n) \to H_1(\tilde{D}_n)$ is the $\mathbb{Z}[q^{\pm 1}]$-module homomorphism induced by $\tilde{\phi}$.
Consider, for all $i = 1, \dots, n-1$, the closed path $w_i := x_i x_{i+1}^{-1} \in \pi_1(D_n, z_*)$. Because w_i lies in $\ker\Phi$, the unique lift $\tilde{w}_i$ is a closed path in $\tilde{D}_n$, and we use the same symbol $\tilde{w}_i$ for the corresponding cycle in $H_1(\tilde{D}_n)$.

Proposition 1.7 *$H_1(\tilde{D}_n)$ is a free $\mathbb{Z}[q^{\pm 1}]$-module of rank $n-1$ with basis $\tilde{w}_1, \dots, \tilde{w}_{n-1}$.*

Proof. - Here we follow the proof sketched in section 2.6 of [**Bi00**]: Observe that D_n is homotopy equivalent to a multigraph with one vertex d (correponding to the base point z_*) and n edges $e_1, \dots, e_n$ (corresponding to the closed paths $x_1, \dots, x_n$). And $\tilde{D}_n$ is homotopy equivalent to a multigraph with vertices $\{q^k d \mid k \in \mathbb{Z}\}$ and edges $\{q^k e_i \mid k \in \mathbb{Z}, i = 1, \ldots, n\}$, where $q^k e_i$ goes from $q^k d$ to $q^{k+1} d$. Denote by W_1 the free $\mathbb{Z}[q^{\pm 1}]$-module with basis $\{e_1, \ldots, e_n\}$, an let W_0 be the free $\mathbb{Z}[q^{\pm 1}]$-module with basis $\{d\}$, then $H_1(\tilde{D}_n)$ is the kernel of the module homomorphism $\partial : W_1 \to W_0$ defined by $e_i \mapsto d$. But this kernel is a free $\mathbb{Z}[q^{\pm 1}]$-module with basis $\{\tilde{w}_1, \ldots, \tilde{w}_{n-1}\}$, where $\tilde{w}_i := e_{i+1} - e_i$. □

Matrices defining the σ_i-action according to this basis were given at the beginning of this section.
An analogue homological definition of the (non-reduced) Burau representation is, e.g., given in [**LP93**, **Tu00**].

A linear representation is called faithful iff it is injective, i.e., it has a trivial kernel. It is known for a long time that the Burau representation is faithful for $n \leq 3$ [**MP69**] (see also Theorem 3.15 in [**Bi74**]). Further, it was regarded as a candidate for a faithful representation of B_n for all n until Moody proved in 1991 [**Mo91**, **Mo93**] that it is not faithful for $n \geq 9$. This result was improved by Long and Paton to all $n \geq 6$ [**LP93**]. A further improvement is due to Bigelow, who found a Burau kernel element in B_5 [**Bi99**]. The case $n = 4$ remains open.
The (reduced) Burau representation is unitary in following sense [**Sq84**]:
Let $M^\dagger$ denote the conjugate-transpose of a matrix M over $\mathbb{T}[q^{\pm 1}]$, where the conjugate of a Laurent polynomial $p(q)$ is defined to be $p(q^{-1})$. Then there exists matrix $J_0 \in GL(n-1, \mathbb{Z}[q^{\pm 1}])$ such that $\beta_{\mathrm{red}}(b)^\dagger J_0 \beta_{\mathrm{red}}(b) = J_0$ for all $b \in B_n$. Further, a change-of-basis leads to (reduced) Burau matrices $\beta'_{\mathrm{red}}(b)$ (for $b \in B_n$) such that the Burau representation is unitary relative to an explicitly defined Hermitian form, i.e., there exists a Hermitian matrix $J \in GL(n-1, \mathbb{Z}[q^{\pm 1}])$ ($J = J^\dagger$), obtained from J_0 by a basis change, such that $\beta'_{\mathrm{red}}(b)^\dagger J \beta'_{\mathrm{red}}(b) = J$ for all $b \in B_n$.

1.3 Lawrence-Krammer representation

In 1990 R. Lawrence gave a topological construction of representations of Hecke algebras associated with 2-row Young diagrams [**La90**]. This construction gives rise to family of representation of B_n. One of these representations was later described algebraically by D. Krammer as a free $\mathbb{Z}[q^{\pm 1}, t^{\pm 1}]$-module generated by the isotopy classes of forks [**Kr00**]:

Definition 1.8 *Recall the notation from definition 1.3. A* fork *(in D_n) is an embedded tree $T \subset D$ with 4 vertices z_*, p_1, p_2, d with $T \cap \mathcal{P} = \{p_1, p_2\}$ and $T \cap \partial D = z_*$, and the 3 edges have d as a vertex. The union of the edges*

containing puncture points is called tine edge of T*, and the third edge is the* handle of T*.*
Two forks T_1, T_2 are said to be isotopic *if there exists a self-homeomorphism $\phi \in H_0$ such that $\phi(T_1) = T_2$. An isotopy class represented by a fork T is denoted by $[T]$.*
If the imaginary part of z is nonnegative for all $z \in T$, i.e., $\Im(z) \geq 0$, then T is called a standard fork*. v_{ij} denotes the isotopy class of a standard fork with punctures i, j.*

We want to introduce the Lawrence-Krammer-module V as a B_n-module with the isotopy classes of forks as generators. The relations between non-isotopic forks in V are determined by the following specific ansatz:

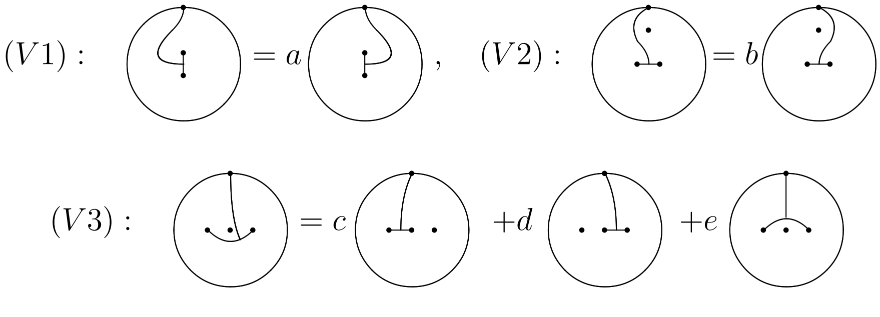


Figure 1.2: Relations between forks

Note that any selfhomeomorphism of D may be applied simultaneously to the disks in figure 1.2. Then the interpretation of B_n as the mapping class group of D_n and a straightforward computation yields the following σ_k-action on standard forks:

$$\begin{array}{rcll}
(\rho\sigma_k)v_{k,k+1} & = & av_{k,k+1}, & \\
(\rho\sigma_k)v_{k+1,j} & = & v_{kj}, & k+1<j, \\
(\rho\sigma_k)v_{kj} & = & -\frac{ca}{e}v_{k,k+1} - \frac{d}{e}v_{kj} + \frac{1}{e}v_{k+1,j}, & k+1<j, \\
(\rho\sigma_k)v_{i,k+1} & = & v_{ik}, & i<k, \\
(\rho\sigma_k)v_{ik} & = & bdv_{k,k+1} + bcv_{ik} + bev_{i,k+1}, & i<k, \\
(\rho\sigma_k)v_{ij} & = & v_{ij}, & \{i,j\} \cap \{k,k+1\} = \emptyset.
\end{array}$$

The commutativity relation $(\sigma_k\sigma_l)v_{kl} = (\sigma_l\sigma_k)v_{kl}$ leads to $b(c+e) = 1$ and $e = 1-d$. And from $(\sigma_k\sigma_{k+1}\sigma_k)v_{k,k+2} = (\sigma_{k+1}\sigma_k\sigma_{k+1})v_{k,k+2}$ we get the following relations for the ansatz parameters: $-d/e = bc, -bc/e = bd, 1/e = be$. It is a straightforward though tedious task to check that in all other cases we do not obtain further relations for the parameters. Setting $q := 1/e$ and $t := ae^2$, we can express the ansatz parameters a, b, c, d, e in terms of q, t.

Definition 1.9 *The* Lawrence-Krammer module V *is defined as the* $\mathbb{Z}[q^{\pm 1}, t^{\pm 1}]$*-module generated by* $\{[T] \mid T$ *is a fork* $\}$ *with defining relations* $(V1) - (V3)$ *and* $a = tq^2$, $b = q^2$, $c = q^{-2} - q^{-1}$, $d = 1 - q^{-1}$, *and* $e = q^{-1}$. *The* Lawrence-Krammer representation *is the mapping* $\rho : B_n \to Aut(V)$ *defined by the above* B_n*-action.*

Proposition 1.10 *The Lawrence-Krammer module* V *is a free* $\mathbb{Z}[q^{\pm 1}, t^{\pm 1}]$*-module of rank* $\binom{n}{2}$ *with basis* $\{v_{ij} \mid 1 \leq i < j \leq n\}$.

Proof. - See Proposition 3.1 in [**Kr00**].

The basis $\{v_{ij} \mid 1 \leq i < j \leq n\}$ is called standard fork basis and ρx $(x \in B_n)$ is identified with its matrix with respect to this basis. Then the matrix elements of an Artin generator are given by $(1 \leq i < k < k+1 < j \leq n)$

$$\begin{array}{rcl}
(\rho\sigma_k)v_{k,k+1} & = & tq^2 v_{k,k+1}, \\
(\rho\sigma_k)v_{k+1,j} & = & v_{kj}, \\
(\rho\sigma_k)v_{kj} & = & tq(q-1)v_{k,k+1} + (1-q)v_{kj} + qv_{k+1,j}, \\
(\rho\sigma_k)v_{i,k+1} & = & v_{ik}, \\
(\rho\sigma_k)v_{ik} & = & q(q-1)v_{k,k+1} + (1-q)v_{ik} + qv_{i,k+1}, \text{ and} \\
(\rho\sigma_k)v_{i_1 i_2} & = & v_{i_1 i_2} \qquad \text{for} \quad \{i_1, i_2\} \cap \{k, k+1\} = \emptyset.
\end{array}$$

Let V^* denote the dual space of V with basis $\{v^*_{ij} \mid 1 \leq i < j \leq n\}$. There exists a natural pairing $\langle \cdot \mid \cdot \rangle : V^* \times V \to \mathbb{Z}[q^{\pm 1}, t^{\pm 1}]$ defined by $\langle v^*_{ij} \mid v_{kl} \rangle = \delta_{ik}\delta_{jl}$, where δ_{ij} denotes the usual Kronecker symbol. Let $\rho^* : B_n \to Aut(V^*)$ be the dual representation defined by $\langle (\rho^* x)v^* \mid v \rangle = \langle v^* \mid (\rho(\operatorname{rev} x))v \rangle$ for all $v^* \in V^*$, $v \in V$ and $x \in B_n$. Here rev : $B_n \to B_n$ is the (reverse) anti-automorphism defined by the identity on the set of Artin generators. Note that $\rho^*(x) = (\rho(\operatorname{rev} x))^\top$.
Then the dual action of an Artin generator on dual standard fork basis elements is described by the transposed matrix, i.e., we have

$$\begin{array}{rcl}
(\rho^*\sigma_k)v^*_{k,k+1} & = & q(q-1)\sum\limits_{i<s} v^*_{ik} + tq^2 v^*_{k,k+1} + tq(q-1)\sum\limits_{k+1<j} v^*_{kj}, \\
(\rho^*\sigma_k)v^*_{ik} & = & (1-q)v^*_{ik} + v^*_{i,k+1}, \\
(\rho^*\sigma_k)v^*_{i,k+1} & = & qv^*_{ik}, \\
(\rho^*\sigma_k)v^*_{kj} & = & (1-q)v^*_{kj} + v^*_{k+1,j}, \\
(\rho^*\sigma_k)v^*_{k+1,j} & = & qv^*_{kj}, \\
(\rho^*\sigma_k)v^*_{i_1 i_2} & = & v^*_{i_1 i_2} \quad \text{for} \quad \{i_1, i_2\} \cap \{k, k+1\} = \emptyset.
\end{array}$$

The dual a_{ts}-action is computed by ($1 \le i_0 < s < j_0 < t < k_0 \le n$)

$$\begin{array}{rcl}
(\rho^* a_{ts})v^*_{st} & = & q(q-1)\sum\limits_{i<s} v^*_{is} + (q-1)^2 \sum\limits_{i<s<j<t} v^*_{ij} + tq(q-1)\sum\limits_{s<j<t} v^*_{jt} \\
 & & +tq^2 v^*_{st} + tq(q-1)\sum\limits_{t<k} v^*_{sk} + t(q-1)^2 \sum\limits_{s<j<t<k} v^*_{jk}, \\
(\rho^* a_{ts})v^*_{i_0 s} & = & (1-q)\sum\limits_{s\le j<t} v^*_{i_0 j} + v^*_{i_0 t}, \\
(\rho^* a_{ts})v^*_{i_0 t} & = & q v^*_{i_0 s} + (q-1)\sum\limits_{s<j<t} v^*_{i_0 j}, \\
(\rho^* a_{ts})v^*_{s j_0} & = & (q-1)\sum\limits_{i<s} v^*_{i j_0} + tq v^*_{j_0 t} + t(q-1)\sum\limits_{t<k} v^*_{j_0 k}, \\
(\rho^* a_{ts})v^*_{j_0 t} & = & t^{-1}(1-q)\sum\limits_{i<s} v^*_{i j_0} + t^{-1} v^*_{s j_0} + (1-q)\sum\limits_{t\le k} v^*_{j_0 k}, \\
(\rho^* a_{ts})v^*_{s k_0} & = & (1-q)\sum\limits_{s\le j<t} v^*_{j k_0} + v^*_{t k_0}, \\
(\rho^* a_{ts})v^*_{t k_0} & = & q v^*_{s k_0} + (q-1)\sum\limits_{s<j<t} v^*_{j k_0}, \\
(\rho^* a_{ts})v^*_{i_1 i_2} & = & v^*_{i_1 i_2} \quad \text{for} \quad \{s,t\} \cap \{i_1, i_2\} = \emptyset.
\end{array}$$

And the transposed matrix describes the rev a_{ts}-action on standard fork basis elements ($1 \le i < s < j < t < k \le n$):

$$\begin{array}{rcl}
(\rho(\mathrm{rev}\, a_{ts}))v_{st} & = & tq^2 v_{st}, \\
(\rho(\mathrm{rev}\, a_{ts}))v_{is} & = & (1-q)v_{is} + q v_{it} + q(q-1)v_{st}, \\
(\rho(\mathrm{rev}\, a_{ts}))v_{it} & = & v_{is}, \\
(\rho(\mathrm{rev}\, a_{ts}))v_{sj} & = & t^{-1} v_{jt}, \\
(\rho(\mathrm{rev}\, a_{ts}))v_{jt} & = & tq v_{sj} + tq(q-1)v_{st} + (1-q)v_{jt}, \\
(\rho(\mathrm{rev}\, a_{ts}))v_{sk} & = & tq(q-1)v_{st} + (1-q)v_{sk} + q v_{tk}, \\
(\rho(\mathrm{rev}\, a_{ts}))v_{tk} & = & v_{sk}, \\
(\rho(\mathrm{rev}\, a_{ts}))v_{ij} & = & (1-q)v_{is} + v_{ij} + (q-1)v_{it} + \\
 & = & (q-1)v_{sj} + (1-q)^2 v_{st} + t^{-1}(1-q)v_{jt}, \\
(\rho(\mathrm{rev}\, a_{ts}))v_{jk} & = & t(q-1)v_{sj} + t(1-q)^2 v_{st} + (1-q)v_{sk} + \\
 & = & (1-q)v_{jt} + v_{jk} + (q-1)v_{tk}, \quad \text{and} \\
(\rho(\mathrm{rev}\, a_{ts}))v_{i_1 i_2} & = & v_{i_1 i_2} \quad \text{for} \quad \{s,t\} \cap \{i_1, i_2\} = \emptyset.
\end{array}$$

The Lawrence-Krammer representation was proved to be faithful for $n = 4$ by D. Krammer in 2000 [**Kr00**]. A slight modification of Krammer's proof is discussed in detail in section 2.3.
Using the forks, introduced by Krammer, S. Bigelow developed a deep topological proof for the faithfulness of the Lawrence-Krammer representation for all $n \in \mathbb{N}$ [**Bi00**, **Bi01**], implying that braid groups are linear[7]. Bigelow's proof can be seen as a converse to the construction of Burau kernel elements

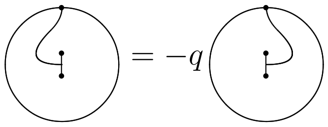
[7] Note that S. Bachmuth claimed the linearity of pure braid groups [**Ba96**], trying to prove the faithfulness of the Gassner representation [**Ga61**]. Nevertheless, his "proof"

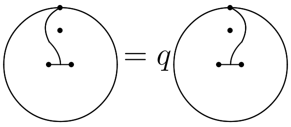
given in [**Mo91**, **LP93**, **Bi99**].
In 2002 Krammer published a combinatorial proof for the faithfulness of the Lawrence-Krammer representation for all $n \in \mathbb{N}$ [**Kr02**]. We review the main steps of this proof in section 2.2.
Further, the Lawrence-Krammer representation ρ is unitary [**So02**], i.e., there exists a matrix $J_1 \in GL(\binom{n}{2}, \mathbb{Z}[q^{\pm 1}, t^{\pm 1}])$ such that $(\rho x)^\dagger J_1(\rho x) = J_1$ holds for all $b \in B_n$.
Murakami [**Mu87**] and, independently, Birman and Wenzl [**BW89**, **We90**], used the skein relations for the Kauffman bracket polynomial [**Ka87**, **Ka93**] to define a new algebra, the BMW algebra. This algebra gives rise to the BMW representation of the braid group B_n, which decomposes into irreducible representations indexed by partitions of $n-2k$ for $0 \leq 2k \leq n$. Jones observed a similarity between the LK representation and a certain summand of the BMW representation. Indeed, following a rescaling and change of parameters, M. Zinno found that the LK representation of B_n is identical to the $(n-2) \times 1$ irreducible representation of the BMW algebra [**Zi01**]. This implies the faithfulness of the BMW algebra and the irreducibility of the Lawrence-Krammer representation.

1.4 The reduced Burau module

As the Lawrence-Krammer representation the (reduced) Burau representation can also be defined by using forks. This leads to an alternative definition of the reduced Burau module W (see [**Kr00**]):

Definition 1.11 *The* reduced Burau module *W is the $\mathbb{Z}[q^{\pm 1}]$-module generated by $\{[T] \mid T$ is a fork $\}$ with relations $(W1) - (W3)$.*

$(W1)$:


$(W2)$:


did not convince the mathematical community (see [**Bi98**]). Indeed, P. Abramenko and T. Müller [**AM99**] presented a counterexample to Bachmuth's main assertion (Theorem C in [**Ba96**]). Further, a detailed analysis [**AM99**] of Bachmuth's proof strategy shows that none of Bachmuth's arguments sheds any light on the question whether the Gassner representation is faithful or not.

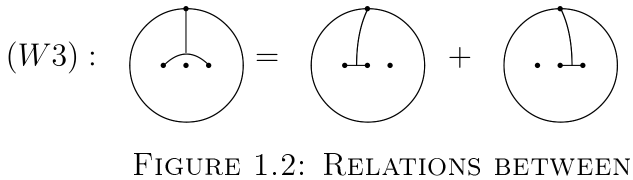


FIGURE 1.2: RELATIONS BETWEEN FORKS IN W

Since there are different relations in W than in V, we use in W the abbreviation w_{ij} for the isotopy class of a standard fork with punctures in i, j instead of v_{ij}. Because of $(W3)$ we have $w_{ij} = \sum_{k=i}^{j-1} w_{k,k+1}$ $(i < j)$. It is easy to show that $\{w_{i,i+1} \mid i = 1, \ldots, n-1\}$ is a basis of W.
Once again, the interpretation of the braid group as a mapping class group leads to a B_n-action on W. The involved representation is the reduced Burau representation $\beta_{\text{red}} : B_n \to Aut(W)$ described in section 1.2, i.e., we have $(j \neq k-1, k, k+1)$:

$$\begin{aligned} (\beta_{\text{red}}\sigma_k)w_{k-1,k} &= w_{k-1,k} + qw_{k,k+1}, & (\beta_{\text{red}}\sigma_k)w_{k,k+1} &= -qw_{k,k+1}, \\ (\beta_{\text{red}}\sigma_k)w_{k+1,k+2} &= w_{k,k+1} + w_{k+1,k+2}, & (\beta_{\text{red}}\sigma_k)w_{j,j+1} &= w_{j,j+1}. \end{aligned}$$

Of course, the map $W \to H_1(\tilde{D}_n)$ defined by $w_{i,i+1} \mapsto \tilde{w}_i$ is an isomorphism of B_n-modules[8].

Definition 1.12 *Let R be a commutative ring and W an R-module. View the tensor product[9] $T = W \otimes_R W$ as an additive written abelian group. Let C be the subgroup of T generated by $v \otimes w - w \otimes v$ for $v, w \in W$. Then the* symmetric square of W, *denoted by S^2W, is defined to be T/C. We use the notation $vw = v \cdot w := v \otimes w = w \otimes v$ and $v^2 = v \cdot v$ for all $v, w \in W$. As T the symmetric square S^2W admits a natural R-module structure, defined by $a(v \otimes w) := (av) \otimes w$ for all $a \in R$ and $v, w \in W$.*

Now, let the coefficient ring of the reduced Burau module W be a commutative ring R where q and 2 are invertible in R. The symmetric square S^2W of the reduced Burau module W is a free R-module with basis $\{w_{ij}^2 \mid 1 \leq i < j \leq n\}$. Note that we can express mixed products as linear combinations of squares $(1 \leq i < j < k < l \leq n)$:

$$\begin{aligned} w_{ij}w_{jk} &= \frac{1}{2}(w_{ik}^2 - w_{ij}^2 - w_{jk}^2), & w_{ij}w_{ik} &= \frac{1}{2}(w_{ij}^2 + w_{ik}^2 - w_{jk}^2), \\ w_{ik}w_{jk} &= \frac{1}{2}(w_{ik}^2 + w_{jk}^2 - w_{ij}^2), & w_{ij}w_{kl} &= \frac{1}{2}(w_{il}^2 + w_{jk}^2 - w_{ik}^2 - w_{jl}^2), \\ w_{ik}w_{jl} &= \frac{1}{2}(w_{il}^2 + w_{jk}^2 - w_{ij}^2 - w_{kl}^2), & w_{il}w_{jk} &= \frac{1}{2}(w_{ik}^2 + w_{jl}^2 - w_{ij}^2 - w_{kl}^2). \end{aligned}$$

[8] Recall that, if G is a group and V is a module or vector space, then V is called a G-module if there exists a group homomorphism $G \to Aut(V)$

[9] Tensor products of modules and algebras are, for example, introduced in [**Hu67**].

The reduced Burau representation $\beta_{\text{red}} : B_n \longrightarrow Aut(W)$ induces a representation $\beta^2 : B_n \longrightarrow Aut(S^2W)$ defined by

$$(\beta^2\sigma_k)w_{ij}^2 := [(\beta_{\text{red}}\sigma_k)w_{ij}]^2 \quad \text{for all} \quad 1 \leq i < j \leq n, \ 1 \leq k < n.$$

Therefore S^2W is also a B_n-module. Using the equations above, we can compute the σ_k-action (induced by the representation β^2) on the basis elements of S^2W:

$$\begin{array}{rcl}
(\beta^2\sigma_k)w_{k,k+1}^2 &=& q^2w_{k,k+1}^2, \\
(\beta^2\sigma_k)w_{k+1,j}^2 &=& w_{kj}^2, \\
(\beta^2\sigma_k)w_{kj}^2 &=& q(q-1)w_{k,k+1}^2 + (1-q)w_{kj}^2 + qw_{k+1,j}^2, \\
(\beta^2\sigma_k)w_{i,k+1}^2 &=& w_{ik}^2, \\
(\beta^2\sigma_k)w_{ik}^2 &=& q(q-1)w_{k,k+1}^2 + (1-q)w_{ik}^2 + qw_{i,k+1}^2, \text{ and} \\
(\beta^2\sigma_k)w_{i_1i_2}^2 &=& w_{i_1i_2}^2 \quad \text{for} \quad \{i_1, i_2\} \cap \{k, k+1\} = \emptyset.
\end{array}$$

Recall the following elementary definition (see, e.g., chapter 1.6 [**Sa01**]).

Definition 1.13 *Let G be a group, and V_1, V_2 are G-modules, i.e., there are homomorphisms $\rho_i : G \longrightarrow Aut(V_i)$ for $i = 1, 2$. A G-homomorphism is a linear transformation $\theta : V_1 \longrightarrow V_2$ which preserves (or respects) the action of G, i.e., it satisfies*

$$\theta((\rho_1g)v) = (\rho_2g)(\theta(v)) \quad \textit{for all} \quad v \in V_1, \ g \in G.$$

Further, a G-isomorphism is a bijective G-homomorphism.

Proposition 1.14 (Proposition 3.2 in [**Kr00**]) *Let R be a commutative ring where q and 2 are invertible elements. Consider the Lawrence-Krammer module V and the symmetric square S^2W of the reduced Burau module over the coefficient ring R.*
The map $\phi : V \longrightarrow S^2W$ given by $v_{ij} \mapsto w_{ij}^2$ is a B_n-isomorphism.

Proof. - Comparing the σ_k-action on the w_{ij}^2's with the σ_k-action induced by the Lawrence-Krammer representation for $t = 1$ (see section 1.3), we observe that

$$\phi((\rho_{t=1}\sigma_k)v) = (\beta^2\sigma_k)(\phi(v)) \quad \text{for all} \quad v \in V, \ k = 1, \ldots, n-1.$$

Since the σ_k's generate B_n, this implies that ϕ is a B_n-homomorphism. Further, the map ϕ is obviously bijective. Hence, the B_n-modules V and S^2W are B_n-isomorphic if $t = 1$. □

1.5 An iterative construction of braid representations

D. D. Long presented in [**Lo94**] a method for constructing new representations from known linear representations of B_n. According to [**BB06**] it is due to Moody, generalizing ideas from [**La90**], and it was first described in [**BLM92**]. This method generalizes the classical construction of Magnus representations [**Bi74**, **Ma74**].

Note that the same method was developed independently in [**L92**, **CL92**, **LT92**], introducing so-called braid-valued representations of B_n. See also [**CT93**, **CL95**, **L96**].

Now we give a short review of the so-called augmenting construction, described in [**Lo94**]: Recall the split exact sequence $F_n \xrightarrow{\alpha} P_{n+1} \xrightarrow{\xi} P_n$, which yields the embedding $P_n \ltimes F_n \cong P_{n+1}$. This sequence naturally extends to the split exact sequence $F_n \xrightarrow{\alpha} B_{n+1}^{(n+1)} \xrightarrow{\xi'} B_n$, where $B_{n+1}^{(n+1)}$ denotes the set of all $b \in B_{n+1}$ with $\nu(b)(n+1) = n+1$. Here the homomorphisms ξ, ξ' are defined by pulling out the $(n+1)$-th braid strand. This extended split exact sequence yields the embedding $B_n \ltimes F_n \cong B_{n+1}^{(n+1)} \subset B_{n+1}$. Thus every representation of B_{n+1} induces (by restriction of the domain) a representation of $F_n \rtimes B_n$. Here B_n acts (from left) on F_n by the induced automorphisms in $\imath(B_n) \subset \mathrm{Aut}(F_n)$:

$$\begin{array}{rcl} B_n \times F_n & \longrightarrow & F_n \\ (b, w) & \longmapsto & {}^b w := \imath(b)(w) = \alpha^{-1}(b\alpha(w)b^{-1}) \end{array}$$

We can extend this B_n-action over the group ring $R[F_n]$, where R denotes a ring with unit 1.

Let I be the right $R[F_n]$-ideal generated by $\{x_i - 1 \mid 1 \leq i \leq n\}$. Then the σ_k-action $(k = 1, \ldots, n-1)$ on $x_i - 1$ is given by

$${}^{\sigma_k}(x_i - 1) = \begin{cases} (x_{k+1} - 1), & i = k, \\ (x_k - 1)x_{k+1} + (x_{k+1} - 1)[1 - x_{k+1}^{-1} x_k x_{k+1}], & i = k+1, \\ (x_i - 1), & i \neq k, k+1. \end{cases}$$

Thus we have ${}^b I \subset I$ (indeed ${}^b I = I$) $\forall b \in B_n$, i.e., B_n operates on I.

If we view I as a right $R[F_n]$-module and the representation space V of a given representation $\rho : F_n \rtimes B_n \to \mathrm{Aut}(V)$ as a left $R[F_n]$-module, then we can define a new representation of B_n by

$$\begin{array}{rcl} \rho^+ : B_n & \longrightarrow & \mathrm{Aut}(I \otimes_{R[F_n]} V), \\ b & \longmapsto & (i \otimes v \mapsto {}^b i \otimes (\rho b)v) \end{array}$$

Defining $V_i := (x_i - 1) \otimes V$, the new representation space can be written as a direct sum of n copies of V:

$$I \otimes_{R[F_n]} V = V_1 \oplus \ldots \oplus V_n \equiv \bigoplus_{i=1}^{n} V_i \cong V^{\oplus n} \equiv V^n.$$

From the σ_i-action on I we compute the $\rho^+(\sigma_i)$-action on $\bigoplus_{i=1}^n V_i \cong V^n$, written in blockmatrix notation, as

$$\rho^+(\sigma_i) = [\mathrm{Id}_V^{\oplus(i-1)} \oplus \begin{pmatrix} 0 & \rho(x_{i+1}) \\ \mathrm{Id}_V & \mathrm{Id}_V - \rho(x_{i+1}^{-1} x_i x_{i+1}) \end{pmatrix} \oplus \mathrm{Id}_V^{\oplus(n-i-1)}]\rho(\sigma_i).$$

In this notation we do not distinguish between x_i and $\alpha(x_i)$.
Analogeously, the σ_k-action $(k = 1, \ldots, n-1)$ on $y_i - 1$ is given by

$$^{\sigma_k}(y_i - 1) = \begin{cases} (y_{k+2} - 1)y_{k+1}^{-1} y_k - (y_{k+1} - 1)y_{k+1}^{-1} y_k + (y_k - 1), & i = k+1 < n, \\ -(y_n - 1)y_n^{-1} y_{n-1} + (y_{n-1} - 1), & i = k+1 = n, \\ (y_i - 1), & i \neq k+1. \end{cases}$$

Let $\bar{I}$ be the right $R[F_n]$-ideal generated by $\{y_i - 1 \mid 1 \leq i \leq n\}$, and let $\bar{\rho}^+ : B_n \to Aut(\bar{I} \otimes_{R[F_n]} V)$ be defined as ρ^+. Further, set $\bar{V}_i := (y_i - 1) \otimes V$. From the σ_i-action on $\bar{I}$ we derive the $\bar{\rho}^+(\sigma_i)$-action on $\bigoplus_{i=1}^n \bar{V}_i \cong V^n$, written in blockmatrix notation, as $(1 \leq i < n-1)$

$$\begin{aligned} \bar{\rho}^+(\sigma_i) &= \rho\sigma_i^{\oplus(i-1)} \oplus \begin{pmatrix} \rho\sigma_i & \rho\sigma_i & 0 \\ 0 & -\rho y_{i+1}^{-1} y_i \sigma_i & 0 \\ 0 & \rho y_{i+1}^{-1} y_i \sigma_i & \rho\sigma_i \end{pmatrix} \oplus \rho\sigma_i^{\oplus(n-i-2)}, \\ \bar{\rho}^+(\sigma_{n-1}) &= \rho\sigma_{n-1}^{\oplus(n-2)} \oplus \begin{pmatrix} \sigma_{n-1} & \rho\sigma_{n-1} \\ 0 & -\rho y_n^{-1} y_{n-1} \sigma_{n-1} \end{pmatrix}. \end{aligned}$$

Further, we can construct a representation, which is similar to ρ^+, by using a slightly different blockmatrix formula:

Theorem 1.15 *Given a representation $\rho : F_n \rtimes B_n \to \mathrm{Aut}(V)$, we may construct a representation $\rho^\ddagger : B_n \to \mathrm{Aut}(V^n)$ defined by*

$$\rho^\ddagger(\sigma_i)) = \rho(\sigma_i)^{\oplus(i-1)} \oplus \mathcal{R}_i^\ddagger \oplus \rho(\sigma_i)^{\oplus(n-i-1)}, \quad \mathcal{R}_i^\ddagger = \begin{pmatrix} 0 & \rho x_{i+1}\sigma_i \\ \rho\sigma_i & \rho\sigma_i - \rho x_{i+1}\sigma_i \end{pmatrix}.$$

Proof. - This is a straightforward computation.

Note that this braid-valued representation does not directly arise from the augmenting construction, described above.

Summarizing, if V is an R-module of rank m, i.e., $V \cong R^m$, we obtain from an m-dimensional representation $\rho : B_{n+1} \to GL(m, R)$ the mn-dimensional representation ρ^+ (or $\rho^\ddagger$ or $\bar{\rho}^+$).

Examples:

1. Let $R = \mathbb{Z}$. Starting with the (one-dim.) trivial representation τ (defined by $\sigma_i \mapsto 1$), we obtain the standard (or "defining") representation of S_n, i.e., the representation of B_n which factors through S_n:

$$\begin{array}{rcl} \tau^+ : B_n & \longrightarrow & GL(n, \mathbb{Z}) \\ \sigma_i & \longmapsto & \mathrm{Id}_{i-1} \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \mathrm{Id}_{n-i-1}. \end{array}$$

2. Let R be the Laurent polynomial ring $\mathbb{Z}[s^{\pm 1}]$ in one variabe s and $\rho : B_{n+1} \to GL(m, \mathbb{Z})$ a given family of representations. Then we can define a one-parameter representation by

$$\rho_s : B_{n+1} \longrightarrow GL(m, \mathbb{Z}[s^{\pm 1}]), \quad \sigma_i \mapsto s \cdot \rho(\sigma_i).$$

   Applying the augmenting construction to ρ_s yields a one-parameter representation ρ_s^+ of B_n which contains more information than ρ^+, i.e. there exist elements $b \in \ker \rho^+$ with $b \notin \ker \rho_s^+$.

   (a) $s^{-1} \cdot \tau_s^+ : B_n \to GL(n, \mathbb{Z}[s^{\pm 1}])$ defined by $\sigma_i \mapsto \mathrm{Id}_{i-1} \oplus \left(\begin{smallmatrix} 0 & s^2 \\ 1 & 1-s^2 \end{smallmatrix}\right) \oplus \mathrm{Id}_{n-i-1}$ is a Burau-type representation.

   (b) Starting with the Burau representation β of B_{n+1}, we get an n^2-dimensional representation $\beta_s^+ : B_n \to GL(n^2, \mathbb{Z}[s^{\pm 1}, t^{\pm 1}])$. This representation can be reduced to the $\binom{n}{2}$-dimensional Lawrence-Krammer representation [**Lo94**]. Indeed, according to Corollary 2.10 in [**Lo94**], iteration of the augmenting construction, beginning with the trivial representation, yields all summands of the Jones representation.

Note that the 2×2 Burau blockmatrix $\left(\begin{smallmatrix} 1-q & q \\ 1 & 0 \end{smallmatrix}\right)$ fulfilles the equation

$$(*)\ (\mathcal{R}^+ \oplus \mathrm{Id}_V)(\mathrm{Id}_V \oplus \mathcal{R}^+)(\mathcal{R}^+ \oplus \mathrm{Id}_V) = (\mathrm{Id}_V \oplus \mathcal{R}^+)(\mathcal{R}^+ \oplus \mathrm{Id}_V)(\mathrm{Id}_V \oplus \mathcal{R}^+).$$

Further, every $\mathcal{R}^+ \in \mathrm{Aut}(V^{\oplus 2}) = GL(2m, R)$ which satisfies this equation gives rise to a linear representation of the braid groups defined by

$$\begin{array}{rcl} \rho(\mathcal{R}^+) : B_n & \longrightarrow & \mathrm{Aut}(V^{\oplus n}) = GL(mn, R) \\ \sigma_i & \longmapsto & \mathrm{Id}_V^{\oplus(i-1)} \oplus \mathcal{R}^+ \oplus \mathrm{Id}_V^{\oplus(n-i-1)}. \end{array}$$

Equation $(*)$ expresses the Artin relations $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ $(i = 1, \ldots, n-1)$, while the far commutativity relations $\sigma_i\sigma_j = \sigma_j\sigma_i$ $\forall |i-j| \geq 2$ are satisfied in the $\rho(\mathcal{R}^+)$-image by construction.

This can be viewed as a direct sum analogue of the well known $\mathcal{R}$-matrix method [**Ji86**], where, given a $\mathcal{R}$-matrix $\mathcal{R} \in \mathrm{Aut}(V^{\otimes 2}) = GL(m^2, R)$, we can introduce the representation

$$\begin{array}{rcl} \rho(\mathcal{R}) : B_n & \longrightarrow & \mathrm{Aut}(V^{\otimes n}) = GL(m^n, R) \\ \sigma_i & \longmapsto & \mathrm{Id}_V^{\otimes(i-1)} \otimes \mathcal{R} \otimes \mathrm{Id}_V^{\otimes(n-i-1)} \end{array}$$

if $\mathcal{R}$ satisfies the famous quantum Yang-Baxter equation

$$(**) \quad (\mathcal{R} \otimes \mathrm{Id}_V)(\mathrm{Id}_V \otimes \mathcal{R})(\mathcal{R} \otimes \mathrm{Id}_V) = (\mathrm{Id}_V \otimes \mathcal{R})(\mathcal{R} \otimes \mathrm{Id}_V)(\mathrm{Id}_V \otimes \mathcal{R}).$$

The theory of quantum groups provides a classification of the solutions to equation $(**)$. In so far all possible $\mathcal{R}$-matrix representations of B_n are known [**Tu88**], while a corresponding classification of the $\mathcal{R}^+$-matrix representations of B_n, i.e. of the solutions of $(*)$, remains open. Here we view just the simple case $m = \dim V = 1$, i.e., $\mathcal{R}^+ = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $ad - bc \neq 0$. In this case equation $(*)$ specifies to

$$\begin{pmatrix} a^2 + bac & ab + bad & b^2 \\ ca + dac & cb + dad & db \\ c^2 & cd & d \end{pmatrix} = \begin{pmatrix} a & ba & b^2 \\ ac & ada + bc & adb + bd \\ c^2 & cda + dc & cdb + d^2 \end{pmatrix}.$$

Thus we have $bad = 0 = dac$. If $b = c = 0$, then $\mathcal{R}^+ = \mathrm{Id}_2$. If $a = 0, d \neq 0$ or $a \neq 0, d = 0$ we obtain with $\mathcal{R}^+ = \left(\begin{smallmatrix} 0 & b \\ c & 1-bc \end{smallmatrix}\right)$ or $\mathcal{R}^+ = \left(\begin{smallmatrix} 1-bc & b \\ c & 0 \end{smallmatrix}\right)$ (generalized) Burau-type representations. And the case $a = d = 0$ yields $\mathcal{R}^+ = \left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right)$, a generalized version of the Tong-Yang-Ma (TYM) [**TYM96**] or standard representation of B_n [**Fo96**].

Chapter 2

Inverting the Lawrence-Krammer representation

2.1 Braid groups and Garside groups

In this section we review the notion of a Garside group [**DP99**] and the solution to the word problem in Garside groups. We start with the definition of two natural partial orders on a monoid.

Definition 2.1 *Let M be a monoid. For $a, b \in M$, we say that a is a* left divisor of b, *or equivalently,* b *is a* right multiple of a, *denoted by $a \prec b$ (or $b \succ a$), if there exists a $c \in M$ with $ac = b$.*
Also we note $a \tilde{\prec} b$ (or $b \tilde{\succ} a$), i.e., a is a right divisor of b *or b is a* left multiple of a *if there exists a $c \in M$ satisfying $b = ca$.*
For $a, b \in M$ we define further

$$\begin{array}{rcl} a \vee b & := & \min_{\prec}\{d \in M \mid a \prec d \ \wedge \ b \prec d\}, \\ a \wedge b & := & \max_{\prec}\{d \in M \mid d \prec a \ \wedge \ d \prec b\}, \\ a \tilde{\vee} b & := & \min_{\tilde{\prec}}\{d \in M \mid d \tilde{\succ} a \ \wedge \ d \tilde{\succ} b\}, \\ a \tilde{\wedge} b & := & \max_{\tilde{\prec}}\{d \in M \mid a \tilde{\succ} d \ \wedge \ b \tilde{\succ} d\}, \end{array}$$

provided these minima and maxima (with respect to $\prec$ and $\tilde{\prec}$) exist. We call $a \vee b$ ($a \tilde{\vee} b$) the least common right (left) multiple *or* right (left) lcm of a and b *and $a \wedge b$ ($a \tilde{\wedge} b$) is the* greatest common left (right) divisor *or* left (right) gcd of a and b.

Definition 2.2 *$a \in M$ is called an* atom *if $a \neq 1$ and $a = bc \Rightarrow (b = 1 \vee c = 1)$.*
M is an atomic monoid *if*

1. *M is generated by its atoms.*

2. *$\forall a \in M \quad \exists N(a) \in \mathbb{N}$: a cannot be written as a product of more than $N(a)$ atoms.*

M is said to be Garside *or a* Garside monoid *if*

1. *M is atomic.*

2. *M is* left *and* right cancellative, *i.e. $\forall a, b, c \in M$: $ca = cb \Rightarrow a = b$ and $ac = bc \Rightarrow a = b$.*

3. *M is a* lcm monoid, *i.e., every pair $(a, b) \in M^2$ admits an unique left and right lcm (and a left and a right gcd).*

4. *There exists an element $\Delta \in M$, called* Garside element, *such that*

   (a) *the left and right divisors of Δ, called* simple elements, *coincide, i.e.,*
   $$\{s \in M \mid s \prec \Delta\} = \{s' \in M \mid \Delta \tilde{\succ} s'\} =: S.$$

   (b) *the simple elements generate M.*

   (c) *S is finite.*

Let G be a group. A submonoid M of G, which is Garside, and its affiliated Garside element Δ provides a Garside structure for *G if G is a group of left and right fractions of M, i.e.,*

$$G = \{ab^{-1} \mid a, b \in M\} = \{a^{-1}b \mid a, b \in M\}.$$

If G admits a Garside structure (M, Δ), then G is called Garside group.

Proposition 2.3 *B_n is a Garside group. It admits natural Garside structures (B_n^+, Δ_n) and (BKL_n^+, δ_n) where B_n^+ and BKL_n^+ denote the monoids generated by the sets $\{\sigma_i \mid i = 1, \ldots, n-1\}$ and $\{a_{ts} \mid 1 \leq s < t \leq n\}$, respectively, and the Garside elements (here also called* fundamental braids*) are*

$$\begin{aligned}\Delta_n &:= \sigma_1(\sigma_2\sigma_1)\ldots(\sigma_{n-1}\sigma_{n-2}\ldots\sigma_1),\\ \delta_n &:= a_{n,n-1}a_{n-1,n-2}\ldots a_{2,1}.\end{aligned}$$

Proof. - For the Garside structure (B_n^+, Δ_n) see [**Th92**]. The dual Garside structure is introduced in [**BKL98**]. □

The simple elements in the Artin presentation, i.e., the left (and right) divisors of Δ_n, are the permutation braids, mentioned in section 1.1. The set of permutation braids will be denoted by Ω. Its cardinality is known to be $n!$. But the set $Q := \{b \in BKL_n^+ \mid b \prec \delta_n\}$ is smaller. Here we have $|Q| = C_n$, where $C_n = \frac{1}{n+1}\binom{2n}{n}$ denotes the n-th Catalan number. The simple elements of the dual presentation, i.e., the elements of Q, are characterised by non-crossing partitions or products of parallel descending cycles [**BKL98**].
We use the notation Ω_1 for the set of Artin generators, and Q_1 for the set of band generators. Let $l_X : B_n \to \mathbb{N}$ denote the length function with respect to the set $X \subset B_n$, i.e., $l_X(b)$ is the smallest number $k \in \mathbb{N}$ such that there exist $x_1, \ldots, x_k \in X \cup X^{-1}$ with $b = x_1 \cdots x_k$. Then the word $x_1 \cdots x_k$ is called geodesic. If $b \in B_n$ is Artin positive (also just called positive) (or BKL positive), i.e., $b \in B_n^+$ (or $b \in BKL_n^+$), then $l_{\Omega_1}(b)$ (or $l_{Q_1}(b)$) is simply given by the word length of any braid word representing b with respect to the alphabet Ω_1 (or Q_1), since the Artin (and the BKL) relations preserve the word lengths. For example, we have $l_{\Omega_1}(\Delta_n) = \binom{n}{2}$ and $l_{Q_1}(\delta_n) = n - 1$. Note that $|\Omega_1| = n - 1$ and $|Q_1| = \binom{n}{2}$. These simple combinatorial observations suggest a kind of duality between the Garside structures (B_n^+, Δ_n) and (BKL_n^+, δ_n), which is extensively explored in [**Be03**].
While the computation of geodesics in the monoids B_n^+, BKL_n^+ is trivial, it was proved by Paterson and Razborov that the set of geodesics (according to the length function $l_{\Omega_1}(\cdot)$) is co-NP-complete [**PR91**], i.e., given a braid word w, the problem to find a shorter word w' representing the same braid is NP-complete. Therefore, unless P=NP, there exists no polynomial algorithm to compute $l_{\Omega_1}(b)$ for a given braid b. Note that this result only holds for a braid group with infinitely many strands, i.e., $\Omega_1 = \{\sigma_1, \sigma_2, \ldots\}$. It is not known whether the same problem is NP-complete for a fixed number of strands n (open question 9.5.6 in [**EC$^+$92**]). Indeed, according to an unpublished preprint by K. Tatsuoka [**Ta87**] cited in [**PR91**], there exists a polynomial time algorithm to produce a geodesic braid word for every fixed n[1]. A linear time algorithm to the minimal word problem for 3-braids is given in [**Be94**]. Further, it would be interesting to investigate analogue questions for the dual length function $l_{Q_1}(\cdot)$.
The Garside structures (B_n^+, Δ_n) and (BKL_n^+, δ_n) are the only known Garside structures in the braid group B_n. Further, it is an open problem whether the pure braid group P_n admits a Garside structure or not. A natural candidate is the monoid generated by the A_{ij}'s with possible Garside element Δ_n^2. Nevertheless, there are many other examples of Garside monoids, e.g, given

[1] Unfortunately we were unable to obtain it. But according to a private communication with Paterson and Razborov there must have been a flaw in that proof.

by Picantin in [**Pi00**, **Pi03**, **Pi05**]: All spherical Artin monoids [**BS72**, **De72**, **Ch92**, **DP99**], Birman-Ko-Lee monoids for spherical Artin groups [**BKL98**, **Be03**, **Pi02**], braid monoids of the complex reflection groups G_7, G_{11}, G_{12}, G_{13}, G_{15}, G_{19} and G_{22} given in [**BMR98**] [**Pi00**], Garside's hypercube monoids [**Ga69**, **Pi00**], monoids for all torus links groups given in [**Pi03**], and some other monoids, arising from the Wirtinger presentation of the link group (see chapter 3 B in [**BZ03**]) of a torus link [**Pi03**], are Garside. M. Picantin proved [**Pi01b**] that every Garside group is an iterated crossed product of Garside groups with an infinite cyclic center. This extends a similar result established independently by Brieskorn and Saito [**BS72**] and by Deligne [**De72**] for sphercal Artin groups. Especially, the center of the braid group B_n is infinite cyclic, generated by $\Delta_n^2 = \delta_n^n$ for $n \geq 3$ [**Ch48**].
Dehornoy proved that, like as braid groups, all Garside groups are torsion free [**De98**, **De04a**].
In Garside groups there exist natural normal forms, the left and right normal form, also called left and right greedy (normal) form, which provide a solution to the word problem in Garside groups.

Proposition 2.4 *G is a Garside group. For every $a \in G$ there exist unique decompositions*

$$a = \Delta^p a_1 \dots a_l, \quad a = \tilde{a}_1 \dots \tilde{a}_{\tilde{l}} \Delta^{\tilde{p}},$$

called left *and* right normal form of *a, where*

1. *$p = \max\{r \in \mathbb{Z} \mid \Delta^{-r} a \in M\}$ and $\tilde{p} = \max\{r \in \mathbb{Z} \mid a\Delta^{-r} \in M\}$.*

2. *the a_i's and $\tilde{a}_i$'s satisfy*

$$\begin{aligned} a_i &= LF(a_{i-1}^{-1} \cdots a_1^{-1} \Delta^{-p} a) = LF(a_i \cdots a_l) \quad \forall i = 1, \dots, l, \\ \tilde{a}_i &= RF(a\Delta^{-\tilde{p}} \tilde{a}_{\tilde{l}}^{-1} \cdots \tilde{a}_{i+1}^{-1}) = RF(\tilde{a}_1 \cdots \tilde{a}_i) \quad \forall i = 1, \dots, \tilde{l}, \end{aligned}$$

with $LF(b) := \Delta \wedge b \in S$, called left most factor of *b, and $RF(b) := \Delta \tilde{\wedge} b \in S$, called the* right most factor of *b.*

Proof. - This is an immediate consequence of the definition of a Garside group and an lcm monoid. □

The map $M \times S \to S$ defined by $(x, y) \mapsto LF(xy)$ is an action of the Garside monoid M on the set of simple elements S. Moreover $LF(xy) = LF(xLF(y))$ holds for all $x, y \in M$.
One can prove that $l = \tilde{l}$ and $p = \tilde{p}$ holds in Garside groups. p, l and $p + l$ are known as the infimum $\inf(a)$, canonical length or gap $cl(a)$, and supremum $\sup(a)$ of a, respectively. Note that $l = cl(a) = l_S(\Delta^{-p} a) = l_S(a_1 \cdots a_l)$.

Further, the minimal word problem in Garside groups with respect to the length function l_S can be solved efficiently. Indeed, the language of geodesics is regular, i.e, it is accepted by a finite-state automaton:

Lemma 2.5 (Lemma 3.7 in [**De02b**]) *Let G be a Garside group with Garside monoid M. For every $g \in G$ there exists an unique decomposition $g = a^{-1}b$ with $a, b \in M$ and $a \wedge b = 1$.*

The left normal forms $a = a_1 \cdots a_j$ and $b = b_1 \cdots b_k$ lead to the decomposition

$$g = a_j^{-1} \cdots a_1^{-1} b_1 \cdots b_k \quad \text{with} \quad a_1, \ldots a_j, b_1, \ldots, b_k \in S.$$

We call this normal form (left) mixed normal form.

Proposition 2.6 [**CM04**] *The mixed normal form yields a geodesic word with respect to l_S for every Garside group G.*

For braid groups and the length functions l_Ω and l_Q such a result was established earlier in [**Ch95**, **Mi99**] and [**Kr00**], respectively.
Let wl be the word length of a braid word representing a given braid, then the computation of the left (or right) normal form needs $O(wl^2 n \log n)$ time in the Artin presentation [**Th92**] and $O(wl^2 n)$ in the BKL presentation [**BKL98**]. Note that the algorithm for computing the left greedy form is reminiscent of the bubble sort algorithm. It needs $O(l^2)$ computations of left gcd's of two simple elements. An implemetation of such lattice operations and the greedy algorithm is described in [**CK$^+$01**].
A quadratic-time algorithm (quadratic in the input length) for the word problem is shared by all automatic groups. Indeed, according to [**De02b**] Garside groups are biautomatic. Roughly speaking, a group is called automatic, if there exists a finite-state automaton which can be used for the computation of the normal form. For the exact definitions of automatic and biautomatic groups see [**EC$^+$92**] or chapter 13 in [**HEO05**].
Recalling $B_n \cong \mathcal{M}(D_n)$, we note that L. Mosher proved that all mapping class groups $\mathcal{M}(\mathcal{S})$ are automatic where $\mathcal{S}$ denotes a compact surface minus a finite, possibly empty set of punctures [**Mo94**, **Mo95**]. The corresponding normal form of an element of $\mathcal{M}(\mathcal{S})$ is called Mosher normal form. For the Mosher normal form of a braid, which, of course, can be computed in quadratic time in the length of the given braid word, see also chapter 8.2 in [**DD$^+$02**].
Other efficient solutions to the word problem in braid groups are provided by

Dehornoy's handle reduction [**De97**], Dynnikov's formulae for a faithful braid action on $\mathbb{Z}^{2n}$ arising from a braid action on laminations [**Dy02**, **DD$^+$02**], Garber, Kaplan and Teicher's algorithm using a braid action on a standard g-base [**GKT02**, **KT03**], and an algorithm from B. Wiest [**Wi02**]. Dehornoy's handle reduction algorithm [**De97**], which turns out to be extremely efficient in practice, will be discussed in section 5.2.4.

2.2 Inverting the Lawrence-Krammer representation in x-basis

Here we view the Lawrence-Krammer representation in a transformed basis $\{x_{ij} \mid 1 \leq i < j \leq n\}$ [**Kr02**], which we call x-basis. The linear transformations between the standard fork basis $\{v_{ij} \mid 1 \leq i < j \leq n\}$ and the new x-basis are given by

$$v_{ij} = x_{ij} + (1-q) \sum_{i<k<j} x_{kj}, \quad x_{ij} = v_j + (q-1) \sum_{i<k<j} q^{k-1-j} v_{kj}.$$

Then the Lawence-Krammer representation induces the following left action of an Artin generator on x-basis elements

$$\sigma_k \cdot x_{ij} := (\rho_n \sigma_k) x_{ij} = \begin{cases} tq^2 x_{k,k+1}, & i=k, j=k+1, \\ (1-q)x_{ik} + qx_{i,k+1}, & i<k=j, \\ x_{ik} + tq^{k-i+1}(q-1)x_{k,k+1}, & i<k, j=k+1, \\ tq(q-1)x_{k,k+1} + qx_{k+1,j}, & i=k, k+1<j, \\ x_{kj} + (1-q)x_{k+1,j}, & i=k+1<j, \\ x_{ij}, & j<k \quad \text{or} \quad k+1<i, \\ x_{ij} + tq^{k-i}(q-1)^2 x_{k,k+1}, & i<k, k+1<j. \end{cases}$$

In order to understand the procedure how to compute the preimage braid $x \in B_n$ from a given LK matrix ρx in x-basis, it is necessary to recapitulate the main steps of the faithfulness proof for the LK representation given by D. Krammer in [**Kr02**].
The following key lemma (Prop. 2.1 in [**Kr02**]) gives a sufficient condition on a B_n-action on any set to be faithful.

Key Lemma 2.7 *Let B_n act (from left) on a set V. This induces a natural action of B_n on the power set 2^V.*
If there exists a family $\{C_y \mid y \in \Omega\}$ of nonempty and pairwise disjoint subsets $C_y \subset V$ such that the inclusion $x \cdot C_y \subset C_{LF(xy)}$ holds for every

$(x,y) \in B_n^+ \times \Omega$, then the B_n-action on V is faithful.

It can be proved by induction that it is sufficient to verify $x \cdot C_y \subset C_{LF(xy)}$ for every $(x,y) \in \Omega_1 \times \Omega$, i.e., one has to verify this inclusion just in a finite number of cases (for a fixed n). Alternatively, one has to show that the inclusion $x \cdot C_y \subset C_{LF(xy)}$ holds for every left greedy pair $(x,y) \in \Omega^2$, i.e. $LF(xy) = x$.
If we specify $q \in (0,1) \subset \mathbb{R}$, the LK module becomes a free R-module with $R = \mathbb{R}[t^{\pm 1}]$. Observe that for $0 < q < 1$ all entries of the matrix $\rho\sigma_k$ are in $\mathbb{R}_{\geq 0} + t\mathbb{R}[t]$. So if we define

$$U := \bigoplus_{i<j} (\mathbb{R}_{\geq 0} + t\mathbb{R}[t])x_{ij} \subset V,$$

this set is invariant under the B_n^+-action, i.e., $B_n^+ U \subset U$. For a subset $A \subset \mathrm{Trp} := \{(i,j) \mid 1 \leq i < j \leq n\}$ we define

$$\begin{aligned} U_A : &= \{\sum_{s \in \mathrm{Trp}} c_s x_s \mid c_s \in \mathbb{R}_{\geq 0} + t\mathbb{R}[t], \quad c_s \in \mathbb{R}[t] \Leftrightarrow s \in A\} \\ &= t\left(\bigoplus_{s \in A} \mathbb{R}[t]x_s\right) \oplus \left(\bigoplus_{s \in \mathrm{Trp}\setminus A} (\mathbb{R}^+ + t\mathbb{R}[t])x_s\right) \\ &= \left(\bigoplus_{s \in \mathrm{Trp}\setminus A} \mathbb{R}^+ x_s\right) \oplus t\left(\bigoplus_{s \in \mathrm{Trp}} \mathbb{R}[t]x_s\right). \end{aligned}$$

In particular we have

$$U_{\mathrm{Trp}} = t\left(\bigoplus_{s \in \mathrm{Trp}} \mathbb{R}[t]x_s\right) \quad \text{and} \quad U_\emptyset = \left(\bigoplus_{s \in \mathrm{Trp}} \mathbb{R}^+ x_s\right) \oplus t\left(\bigoplus_{s \in \mathrm{Trp}} \mathbb{R}[t]x_s\right).$$

U is the disjoint union $\biguplus_{A \in 2^{\mathrm{Trp}}} U_A$. For any $A \subset \mathrm{Trp}$ and $x \in B_n^+$ there exists an unique $B \subset \mathrm{Trp}$ with $xU_A \subset U_B$, denoted by $B = xA$. Thus we have an action of B_n^+ on 2^{Trp}, defined by $B_n^+ \times 2^{\mathrm{Trp}} \to 2^{\mathrm{Trp}}$, $(x,A) \mapsto xA$.
Note that $x\emptyset$ contains all indices $s \in \mathrm{Trp}$ of rows of ρx such that all entries in these rows are in $t\mathbb{R}[t]$, i.e. for $t = 0$ $x\emptyset$ indicates zero rows in $\rho x|_{t=0}$.

Definition 2.8 *$A \subset \mathrm{Trp}$ is called a* half-permutation *if*

$$\forall\ 1 \leq i < j < k \leq n : \quad (i,j) \in A \ \wedge \ (j,k) \in A \Rightarrow (i,k) \in A.$$

$\mathrm{HP} \subset 2^{\mathrm{Trp}}$ denotes the set of half-permutations.

Proposition 2.9 (Lemma 4.2 in [**Kr02**]) HP *is B_n^+-invariant, i.e.* $A \in \mathrm{HP} \Rightarrow xA \in \mathrm{HP}$.

We define an obviously injective map $L : S_n \to 2^{\mathrm{Trp}}$ by

$$L(\tau) := \{(i,j) \mid 1 \leq i < j \leq n, \quad \tau(i) > \tau(j)\}.$$

Note that $|L(\tau)| = |\tau|$ and $L(\tau) \in \mathrm{HP}$ for all $\tau \in S_n$. Further, we have $\forall A \subset \mathrm{Trp}$

$$A \in L(S_n) \quad \Leftrightarrow \quad A \in \mathrm{HP} \ \wedge \ \bar{A} := \mathrm{Trp} \setminus A \in \mathrm{HP}, \quad \text{and}$$

$$x \prec y \Leftrightarrow L(\nu(x)) \subset L(\nu(y)) \quad \forall x, y \in \Omega.$$

Proposition 2.10 (Lemma 4.3 in [**Kr02**]) *For every* $A \in \mathrm{HP}$ *there exists a greatest (with respect to inclusion)* $B \in L(S_n)$ *with* $B \subset A$*, denoted by* $B = \mathrm{Proj}(A)$.

Proposition 2.11 (Lemma 4.4 in [**Kr02**]) *The map (Greatest Braid)* $GB := \nu^{-1} \circ L^{-1} \circ \mathrm{Proj} : \mathrm{HP} \to \Omega$ *is B_n^+-equivariant, i.e., the following diagram commutes*

$$\begin{tikzcd}
A \arrow[d, mapsto] & \mathrm{HP} \arrow[r, "GB"] \arrow[d] & \Omega \arrow[d] & y = GB(A) \arrow[d, mapsto] \\
xA & \mathrm{HP} \arrow[r, "GB"] & \Omega & LF(xy) = GB(xA).
\end{tikzcd}$$

In formula we have $GB(xA) = LF(xGB(A))$ *for all* $x \in B_n^+$ *and* $A \in \mathrm{HP}$.

Theorem 2.12 (Lemma 4.6 in [**Kr02**]) *The Lawrence-Krammer representation* $\rho : B_n \to GL(\binom{n}{2}, \mathbb{Z}[q^{\pm 1}, t^{\pm 1}])$ *is faithful, even if we specify* $q \in (0,1)$.

Proof. - For $y \in \Omega$, define $C_y := \bigcup_{A \in GB^{-1}(y)} U_A \subset V$. Since the sets $\{U_A\}_{A \in \mathrm{HP}}$ are disjoint, the sets $\{C_y\}_{y \in \Omega}$ are disjoint, too. The sets $\{C_x\}_{x \in \Omega}$ are non-empty because of $\emptyset \neq U_{L(\nu(y))} \subset C_y$. It remains to prove that $xC_y \subset C_{LF(xy)}$ $\forall (x,y) \in B_n^+ \times \Omega$. Since $C_y = \bigcup \{U_A \mid A \in \mathrm{HP}, GB(A) = y\}$, it suffices to show $xU_A \subset C_{LF(xy)}$ for all $A \in \mathrm{HP}$ with $GB(A) = y$. We get the following chain of inclusions:

$$xU_A \subset U_{xA} \subset C_{GB(xA)} = C_{LF(xy)}.$$

The first inclusion is an immediate consequence of the definition of the B_n^+-action on 2^{Trp}, i.e., the definition of xA. By Prop. 2.9 xA is a half-permutation. So, by Prop. 2.10 $\mathrm{Proj}(A)$ and $GB(A)$ are defined, and we get the second inclusion. The last equality follows from the B_n^+-equivariance of GB.
Thus the sets $\{C_y\}_{y\in\Omega}$ fulfill all conditions of the key lemma 2.7 and the proof is finished. □

Note that the following diagrams commute:

$$\begin{tikzcd}
v \in U_A \arrow[d, mapsto] & U \arrow[d] & \biguplus\limits_{A\in\mathrm{HP}} U_A \arrow[l, hook'] \arrow[r, "\mathrm{id}"] \arrow[d] & \biguplus\limits_{x\in\Omega} C_x \arrow[d] & v \in C_x \arrow[d, mapsto] \\
A & 2^{\mathrm{Trp}} & \mathrm{HP} \arrow[l, hook'] \arrow[r, "GB"] & \Omega & x
\end{tikzcd}$$

Krammer's faithfulness proof [**Kr00**] has been generalised by Cohen and Wales [**CW02**], and Digne [**Di03**] to a proof for the linearity of all Artin groups.
An explicit algorithm for inverting the Lawrence-Krammer representation in x-basis is given in section 2.4.

2.3 Inverting the Lawrence-Krammer representation in standard fork basis

Here we describe an algorithm for computing preimage braids directly in the Garside normal form of the dual presentation, given a LK matrix in standard fork basis. To understand this algorithm it is necessary to review the main steps of D. Krammers proof of the linearity of B_4 [**Kr00**]. Nevertheless we will present here a slightly diffferent proof.
Different to section 2.2., here we specify $t \in (0,1) \subset \mathbb{R}$, so that the LK module V becomes a free R-module with $R = \mathbb{R}[q^{\pm 1}]$.

2.3.1 Motivation

The formulas given in section 1.3. imply that $\rho^* x \in Mat(\binom{n}{2}, \mathbb{Z}[q, t^{\pm 1}])$ for all $x \in BKL_n^+$, i.e., $\rho^* x$ has no poles in $q = 0$ for $x \in BKL_n^+$. Define the monoid representation $\rho_0 : BKL_n^+ \to GL(\binom{n}{2}, \mathbb{Z}[t^{\pm 1}])$ by $\rho_0 x := (\rho x) \mid_{q=0}$.

Then we have

$$\begin{array}{rcl}
(\rho_0^* a_{ts})v_{st}^* &=& \sum\limits_{i<s<j<t} v_{ij}^* + tq^2 v_{st}^* + t \sum\limits_{s<j<t<k} v_{jk}^*, \\
(\rho_0^* a_{ts})v_{i_0 s}^* &=& \sum\limits_{s\le j\le t} v_{i_0 j}^*, \\
(\rho_0^* a_{ts})v_{i_0 t}^* &=& -\sum\limits_{s<j<t} v_{i_0 j}^*, \\
(\rho_0^* a_{ts})v_{s j_0}^* &=& -\sum\limits_{i<s} v_{i j_0}^* - t \sum\limits_{t<k} v_{j_0 k}^*, \\
(\rho_0^* a_{ts})v_{j_0 t}^* &=& t^{-1} \sum\limits_{i\le s} v_{i j_0}^* + \sum\limits_{t\le k} v_{j_0 k}^*, \\
(\rho_0^* a_{ts})v_{s k_0}^* &=& \sum\limits_{s\le j\le t} v_{j k_0}^*, \\
(\rho_0^* a_{ts})v_{t k_0}^* &=& -\sum\limits_{s<j<t} v_{j k_0}^*, \\
(\rho_0^* a_{ts})v_{i_1 i_2}^* &=& v_{i_1 i_2}^* \quad \text{for} \quad \{s,t\} \cap \{i_1, i_2\} = \emptyset,
\end{array}$$

and

$$\begin{array}{rcl}
(\rho_0(\operatorname{rev} a_{ts}))v_{st} &=& 0, \\
(\rho_0(\operatorname{rev} a_{ts}))v_{is} &=& v_{is}, \\
(\rho_0(\operatorname{rev} a_{ts}))v_{it} &=& v_{is}, \\
(\rho_0(\operatorname{rev} a_{ts}))v_{sj} &=& t^{-1} v_{jt}, \\
(\rho_0(\operatorname{rev} a_{ts}))v_{jt} &=& v_{jt}, \\
(\rho_0(\operatorname{rev} a_{ts}))v_{sk} &=& v_{sk}, \\
(\rho_0(\operatorname{rev} a_{ts}))v_{tk} &=& v_{sk}, \\
(\rho_0(\operatorname{rev} a_{ts}))v_{ij} &=& v_{is} + v_{ij} - v_{it} - v_{sj} + v_{st} + t^{-1} v_{jt}, \\
(\rho_0(\operatorname{rev} a_{ts}))v_{jk} &=& -tv_{sj} + tv_{st} + v_{sk} + v_{jt} + v_{jk} - v_{tk}, \quad \text{and} \\
(\rho_0(\operatorname{rev} a_{ts}))v_{i_1 i_2} &=& v_{i_1 i_2} \quad \text{for} \quad \{s,t\} \cap \{i_1, i_2\} = \emptyset.
\end{array}$$

This allows us to make the following observation.

Theorem 2.13 *$\forall x \in Q$: $\rho_0^* x$ is a projector, i.e., $(\rho_0^* x)^2 = \rho_0^* x$.*

PROOF. - The proof is done by induction over $l_{Q_1}(x)$:

1. $l_{Q_1}(x) = 1$: It is straightforward to verify $(\rho_0^* a_{ts})^2 = \rho_0^* a_{ts}$ for $1 \le s < t \le n$.

2. $l_{Q_1}(x) > 1$: Recall the definitions of starting and finishing sets of a BKL positive braid b from [**BKL98**]:

$$\begin{array}{rcl}
S(b) &:=& \{a \in Q_1 \mid \exists b' \in BKL_n^+ :\ b = ab'\}, \\
F(b) &:=& \{a \in Q_1 \mid \exists b' \in BKL_n^+ :\ b = b'a\}.
\end{array}$$

According to corollary 3.7 (IV) in [**BKL98**], we have $S(x) = F(x)$ for all $x \in Q$. Now, let a_{ts} be in $S(x) = F(x)$. This implies $x = a_{ts}x' = x''a_{ts}$ for some $x', x'' \in Q$. Then we have

$$\rho_0^*x = \rho_0^*a_{ts}(\rho_0^*x') \overset{!}{=} \rho_0^*a_{ts}x'^2 = \rho_0^*x''a_{ts}x' \overset{1.}{=} \rho_0^*x''\rho_0^*a_{ts}^2x' = \rho_0^*x^2. \quad \square$$

The eigenspaces for the eigenvalues $\lambda = 1, 0$ of $\rho_0^*a_{ts}$, i.e., the image and the kernel under this monoid representation, respectively, are given by

$$\begin{aligned}
\mathrm{im}(\rho_0^*a_{ts}) &= \{v^* \in V^* \mid (\rho_0^*a_{ts})v^* = v^*\} \\
&= \{\sum_{i<j} d_{ij}v_{ij}^* \mid d_{st} = 0,\ d_{is} = d_{it} \quad \forall i < s, \\
&\qquad d_{sj} = t^{-1}d_{jt} \quad \forall s < j < t,\ d_{sk} = d_{tk} \quad \forall t < k\}, \\
\ker(\rho_0^*a_{ts}) &= \{v^* \in V^* \mid (\rho_0^*a_{ts})v^* = 0\} \\
&= \{\sum_{i<j} d_{ij}v_{ij}^* \mid d_{is} = 0 \quad \forall i < s,\ d_{jt} = 0 \quad \forall s < j < t, \\
&\qquad d_{sk} = 0 \quad \forall t < k,\ d_{ij} + d_{st} = d_{it} + d_{sj} \quad \forall i < s < j < t, \\
&\qquad td_{st} + d_{jk} = td_{sj} + d_{tk} \quad \forall s < j < t < k\}.
\end{aligned}$$

Note that $V \cong V^*$ since V is finite-dimensional.
The structure of the image and the kernel of a simple element $x \in Q$ with $l_{Q_1}(x) = k > 1$ is determined by the following theorem.

Theorem 2.14 *Let be $x = a_1 \cdots a_k \in Q$ with $a_1, \ldots, a_k \in Q_1$. Then we have*

$$\mathrm{im}(\rho_0^*a_1 \cdots a_k) = \bigcap_{i=1}^{k} \mathrm{im}(\rho_0^*a_i) \quad \text{and} \quad \ker(\rho_0^*a_1 \cdots a_k) = \sum_{i=1}^{k} \ker(\rho_0^*a_i).$$

Proof. - Let $A, B \in Mat(N, R)$ ($N \in \mathbb{N}$, R ring) be idempotent matrices, i.e. $A^2 = A$ and $B^2 = B$. Choose an $x \in \mathrm{im}(A) \cap \mathrm{im}(B)$. Then there exist $v, v' \in R^N$ with $x = Av = A^2v = Ax = ABv'$. This implies $\mathrm{im}(A) \cap \mathrm{im}(B) \subset \mathrm{im}(AB)$.
Especially for $x = a_{ts}x' = x''a_{ts}$ and $A_{ts} := \rho_0^*a_{ts}$, $X := \rho_0^*x$, $X' := \rho_0^*x'$ and $X'' := \rho_0^*x''$, we have

$$\mathrm{im}(A_{ts}) \cap \mathrm{im}(X') \subset \mathrm{im}(X) \quad \text{and} \quad \mathrm{im}(X'') \cap \mathrm{im}(A_{ts}) \subset \mathrm{im}(X).$$

Since $\mathrm{im}(X) = \mathrm{im}(X''A_{ts}) \subset \mathrm{im}(X'')$ and $\mathrm{im}(X) = \mathrm{im}(A_{ts}X') \subset \mathrm{im}(A_{ts})$ the opposite of the second inclusion holds, too. Therefore we have

$$\mathrm{im}(X'') \cap \mathrm{im}(A_{ts}) = \mathrm{im}(X''A_{ts}) = \mathrm{im}(X),$$

and the first assertion is proved by induction over $l_{Q_1}(x)$. $\square$

Since $\mathrm{im}(A) \supset \mathrm{im}(AC)$ the map

$$\begin{array}{rcl} (Q, \prec) & \longrightarrow & (2^{V^*}, \subset) \quad \text{defined by} \\ a_{ts} & \longmapsto & \mathrm{im}(\rho_0^* a_{ts}) = \rho_0^* a_{ts}(V^*) \end{array}$$

is an order-reversing injection.

Lemma 2.15 *A braid action $\rho : B_n \times V \to V$, e.g., defined by an linear representation ρ , induces a BKL_n^+-action $\rho_0 : BKL_n^+ \times V \to V$, i.e., $\rho x v = \rho y v \Rightarrow \rho_0 x v = \rho_0 y v$ for all $x, y \in BKL_n^+$ and $v \in V$. This naturally induces a BKL_n^+-action $\rho_0 : BKL_n^+ \times 2^V \to 2^V$.*
If there exist a bijection between Q and $\tilde{Q} := \{C_y \subset V \mid y \in Q\}$, and BKL_n^+ acts on $\tilde{Q}$ via ρ_0 with

$$\rho_0 x C_y = C_{LF(xy)} \quad \forall x \in BKL_n^+, y \in Q,$$

then the B_n-action ρ is faithful.

Proof. - Since $\forall z \in B_n \, \exists x, y \in BKL_n^+ : z = xy^{-1}$ it suffices to show $\rho x = \rho y \Rightarrow x = y$, which will be proved by induction over $l_Q(x)$.
The case $l_Q(x) = 1$ is given by the bijection $Q \xrightarrow{\sim} \tilde{Q}$.
In the case $l_Q(x) > 1$ we have

$$\rho x = \rho y \Rightarrow C_{LF(x)} = \rho_0 x C_e = \rho_0 y C_e = C_{LF(y)} \Rightarrow LF(x) = LF(y).$$

Write $x = LF(x)x'$ and $y = LF(x)y'$, then we have

$$(\rho LF(x))\rho x' = (\rho LF(x))\rho y \Leftrightarrow \rho x' = \rho y' \overset{!}{\Rightarrow} x' = y' \Rightarrow x = y. \quad \square$$

Once again, it suffices to show $\rho_0 x C_y = C_{LF(xy)}$ for all $(x, y) \in Q_1 \times Q$.

Lemma 2.16 *Let $\cdot$ be a BKL_n^+-action on $\tilde{Q}$.*

$x \cdot C_y = C_{LF(xy)} \; \forall (x, y) \in Q_1 \times Q \;\; \Rightarrow \;\; x \cdot C_y = C_{LF(xy)} \; \forall (x, y) \in BKL_n^+ \times Q.$

Proof. - Induction over $|x| := l_{Q_1}(x)$.
For $|x| = 1$ there is nothing to prove. Let $x = uv$ with $|u|, |v| < |x|$.

$$x \cdot C_y = u \cdot (v \cdot C_y) \overset{!}{=} u \cdot C_{LF(vy)} \overset{!}{=} C_{LF(uLF(vy))} = C_{LF(u(vy)} = C_{LF(xy)}. \quad \square$$

We use this lemma to obtain a first faithfulness result for $n = 3$.

Corollary 2.17 *The Lawrence-Krammer representation $\rho : B_3 \to GL(3, R)$ with $R = \mathbb{R}[q^{\pm 1}]$ is injective for each $t \in \mathbb{R}$.*

PROOF. - Consider the natural BKL_n^+-action on 2^{V^*} defined by $x \cdot C := (\rho_0^*)C$, which is induced by the dual Lawrence-Krammer representation ρ^* via $\rho_0^* := \rho^*|_{q=0}$. Define $\tilde{Q} := \{C_y := \mathrm{im}(\rho_0^* y) \mid y \in Q\}$.
Explicitly we have $\rho_0^* e = \mathrm{id}_3$, $C_e = V^*$, and $\rho_0^* \delta_3 = (0)_3$, $C_{\delta_3} = \{0\}$, and

$$\rho_0^* a_{21} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \qquad C_{a_{21}} = \{ \begin{pmatrix} 0 \\ \beta \\ \beta \end{pmatrix} \mid \beta \in \mathbb{R}\}, \text{ and}$$

$$\rho_0^* a_{31} = \begin{pmatrix} 0 & 0 & t^{-1} \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad C_{a_{31}} = \{ \begin{pmatrix} t^{-1}\gamma \\ 0 \\ \gamma \end{pmatrix} \mid \gamma \in \mathbb{R}\}, \text{ and}$$

$$\rho_0^* a_{32} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad C_{a_{32}} = \{ \begin{pmatrix} \alpha \\ \alpha \\ 0 \end{pmatrix} \mid \alpha \in \mathbb{R}\},$$

according to the ordered basis $\{v_{12}^*, v_{13}^*, v_{23}^*\}$.
It is easy to check that BKL_n^+ acts on $\tilde{Q}$ with $a \cdot C_y = C_{LF(ay)}$ for all $Q_1 \times Q$, i.e., the preconditions of the lemmata 2.15 and 2.16 are fulfilled. □

Note that if we set $t = 1$, this implies the faithfulness of the Burau representation for $n = 3$.
For $n = 4$ this method does not work. Here we have just $a \cdot C_y = C_{LF(ay)}$ for all $(a, y) \in (Q_1 \times Q) \setminus \{(a_{42}, a_{41}a_{32}), (a_{31}, a_{43}a_{21})\}$. In the first counterexample we have for $v \in C_{a_{41}a_{32}}$

$$a_{42} \cdot v = (\rho_0^* a_{42})v = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & -1 & -1 & 1 & t^{-1} \\ 0 & 0 & 0 & 0 & 0 & t^{-1} \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \alpha \\ 0 \\ 0 \\ t\alpha \\ t\alpha \end{pmatrix} = \begin{pmatrix} \alpha \\ (3+t)\alpha \\ \alpha \\ \alpha \\ 0 \\ t\alpha \end{pmatrix}.$$

This implies $a_{42} \cdot C_{a_{41}a_{32}} \subsetneq C_{LF(a_{42}a_{41}a_{32})} = C_{a_{42}} = \{(\alpha, \beta, \gamma, \alpha, 0, t\gamma)^\top \mid \alpha, \beta, \gamma \in \mathbb{R}\}$.
Since $LF(x) \prec x \ \forall x \in BKL_n^+$ the inclusion $x \cdot C_y = (\rho_0^* x)\rho_0^* y V^* = (\rho_0^* xy)V^* \subset \rho_0^*(LF(xy))V^* = C_{LF(xy)}$ with $(x, y) \in BKL_n^+ \times Q$ holds for all $n \in \mathbb{N}$.
In order to apply this inclusion for a faithfulness proof of the Lawrence-Krammer representation it is necessary to define proper nonempty, disjoint

subsets of $\mathrm{im}(\rho_0^* y)$, $y \in Q$, and use the following variant of a lemma of D. Krammer (Proposition 5.1 in [**Kr00**]).

Main Lemma 2.18 *A braid action $\rho : B_n \times V \to V$, e.g., defined by an linear representation ρ, induces a BKL_n^+-action $\rho_0 : BKL_n^+ \times V \to V$ with $\rho_0 x = \rho_0 y \Rightarrow x = y$. This naturally induces a BKL_n^+-action $\rho_0 : BKL_n^+ \times 2^V \to 2^V$. If there exists a family $\{C_y \mid y \in Q\}$ of nonempty and pairwise disjoint subsets $C_y \subset V$ such that the inclusion $\rho_0 x C_y \subset C_{LF(xy)}$ holds for every $(x, y) \in BKL_n^+ \times Q$, then the B_n-action on V is faithful.*

Proof. - Once again it suffices to show $\rho x = \rho y \Rightarrow x = y$ for all $x, y \in BKL_n^+$, which will be proved by induction over $l_Q(x)$.
$l_Q(x) = 1 :\quad \rho x = \rho y \Rightarrow \rho_0 x = \rho_0 y \Rightarrow x = y.$
$l_Q(x) > 1$: Choose a $v \in C_e$. Then we have

$$\rho_0 x v = \rho_0 y v \in C_{LF(x)} \cap C_{LF(y)} = \begin{cases} \emptyset & LF(x) \neq LF(y) \\ C_{LF(x)} \neq \emptyset & LF(x) = LF(y) \end{cases},$$

which implies $LF(x) = LF(y)$, and the assertion follows by induction. □

Note that it suffices to verify $\rho_0 x C_y \subset C_{LF(xy)}$ for all $(x, y) \in Q_1 \times Q$, or equivalently, $\rho_0 x C_y \subset C_x$ for all left greedy pairs $(x, y) \in Q^2$.

2.3.2 On some special distance spaces

A classical reference on distance geometry is [**Bl53**]. We refer to [**DL97**] and the notation therein.

Definition 2.19 *A* distance space *is a pair (X, d) with a set X and a symmetric function, called distance, $d : X^2 \to \mathbb{R}$ with $d(i, j) \geq 0\ \forall i, j \in X$ and $i = j \Rightarrow d(i, j) = 0$.*

Here view finite distance spaces, i.e., $X \cong V_n := \{1, \ldots, n\}$ for some $n \in \mathbb{N}$. The $n \times n$ symmetrc matrix D, whose (i, j)-th entry is $d_{ij} := d(i, j)\,\forall i, j \in V_n$, is the distance matrix of the finite distance space (V_n, d). Since $d_{ij} = d_{ji}\,\forall i, j \in V_n$ and $d_{ii} = 0\,\forall i \in V_n$, the distance d is given by its restriction on $E_n := \{(i, j) \in V_n^2 \mid 1 \leq i < j \leq n\}$. So d can be viewed as vector $(d_{ij})_{1 \leq i < j \leq n} \in \mathbb{R}^{E_n} \cong \mathbb{R}^{\binom{n}{2}}$.

Definition 2.20 *If a distance d satisfies the* triangle inequalities

$$d(i, k) \leq d(i, j) + d(j, k) \quad \forall i, j, k \in X,$$

then d is called a semimetric *on X, and if, in addition, $d(i,j) = 0 \Rightarrow i = j$, then d is a* metric.
The cone

$$C_n^{SM} := \{d \in \mathbb{R}^{E_n} \mid d \textit{ is a semimetric on } V_n\}$$

is called semimetric cone.

For any $p \geq 1$, we can define the l_p-metric on the vector space $\mathbb{R}^m$ as the associated norm metric of the well-known l_p-norm:

$$d_{l_p}(x,y) := ||x||_p = (\sum_{k=1}^{m} |x_k - y_k|^p)^{1/p}.$$

We use the notation abbreviation $l_p^m = (\mathbb{R}^m, d_{l_p})$.

Definition 2.21 *A distance space (X,d) is said to be* (isometrically) embeddable *into another distance space (X', d') if there exists a mapping $\phi : X \to X'$ such that $d(i,j) = d'(\phi(i), \phi(j))$ for all $i, j \in X$.*
*And (X,d) is said to be l_p-*embeddable *if it is embeddable into l_p^m for some $m \in \mathbb{N}$.*

We are interested in l_2-embeddable (or euclidean) distance spaces. We recall some classical results on l_2-embeddability:
The first result is due to Schoenberg [**Sc35**, **Sc38**].

Definition 2.22 *Let $b \in \mathbb{Z}^n$. The inequality $Q_n(b)^\top d := \sum_{1 \leq i < j \leq n} b_i b_j d_{ij} \leq 0$ is said to be of* negative type *if $\sum_{i=1}^n b_i = 0$. It is* pure *if $|b_i| = 0, 1$ for all $i \in V_n$, and if $\sum_{i=1}^n |b_i| = 2k$ holds for some $k \in \mathbb{N}$, then it is called a k-*gonal inequality.
The negative type cone *is defined by*

$$C_n^{\text{neg}} := \{d \in \mathbb{R}^{E_n} \mid \sum_{1 \leq i < j \leq n} b_i b_j d_{ij} \leq 0 \quad \forall b \in \mathbb{Z}^n \text{ with } \sum_{i=1}^{n} b_i = 0\}.$$

Proposition 2.23 (Theorem 6.2.2 in [**DL97**]) *The distance space $(X, \sqrt{d})$ is l_2-embeddable iff (X,d) is of negative type.*

Alternatively, define the euclidean cone as

$$C_n^{\text{eucl}} := \{d \in \mathbb{R}^{E_n} \mid \sqrt{d} \text{ is } l_2\text{−embeddable}\},$$

then Prop. 2.23 can be restated as $C_n^{\text{eucl}} = C_n^{\text{neg}}$.

The second characterization of euclidicity is due to Gower [**Go82**].

Proposition 2.24 *(X, d) is of negative type if and only if the matrix $A=(\text{id}_n - es^\top)(-D)(\text{id}_n - se^\top)$ is positive semidefinite for any $s \in \mathbb{R}^n$ with $s^\top e = 1$, where e denotes the all-ones column vector.*

A further result, formulated in terms of Cayley-Menger determinants, is due to Menger [**Me28**, **Me31**, **Me54**]. In this explicit form it appears in [**Me54**] or [**DL97**].

Definition 2.25 *Let (X, d) be a finite distance space with $|X| = n$. Then the* Caley-Menger matrix *is defined as the $(n+1) \times (n+1)$ symmetric matrix*

$$CM(X,d) := \begin{pmatrix} D & e \\ e^\top & 0 \end{pmatrix},$$

and $\det CM(X,d)$ denotes its Cayley-Menger determinant.

Proposition 2.26 *$(V_n, \sqrt{d})$ is l_2-embeddable iff $(-1)^{|Y|} \det CM(Y,d) \geq 0$ for all $Y \subset V_n$.*

For $|Y| = 2$, i.e., $Y = \{i, j\}$ with $i < j$, we get $\det CM(Y,d) = 2d_{ij} \geq 0$. For $|Y| = 3$, i.e., $Y = \{i, j, k\}$ with $i < j < k$, we get

$$\begin{aligned} 0 \ \geq\ & \det CM(Y,d) = d_{ij}^2 + d_{ik}^2 + d_{jk}^2 - 2d_{ij}d_{ik} - 2d_{ij}d_{jk} - 2d_{ik}d_{jk} \\ =\ & (\sqrt{d_{ij}} + \sqrt{d_{ik}} + \sqrt{d_{jk}})(\sqrt{d_{ij}} - \sqrt{d_{ik}} - \sqrt{d_{jk}}) \cdot \\ & (-\sqrt{d_{ij}} + \sqrt{d_{ik}} - \sqrt{d_{jk}})(-\sqrt{d_{ij}} - \sqrt{d_{ik}} + \sqrt{d_{jk}}). \end{aligned}$$

Hence, (V_3, d) is euclidean if and only if d satisfies the triangle inequalities, i.e., (V_3, d) is a semimetric space.
So, if we define the following variant of the semimetric cone

$$C_n^{\sqrt{SM}} := \{d \in \mathbb{R}^{E_n} \mid \sqrt{d} \text{ is a semimetric on } V_n\},$$

we get

$$C_3^{\text{eucl}} = C_3^{\sqrt{SM}} \quad \text{and} \quad C_n^{\text{eucl}} \subset C_n^{\sqrt{SM}} \quad \forall n \in \mathbb{N}.$$

Further, $(V_4, \sqrt{d})$ is l_2-embeddable iff it is semimetric and

$$\begin{aligned} 0 \ &\leq\ \det CM(V_4, d) \\ &=\ 2(-d_{12}^2 d_{34} - d_{12} d_{34}^2 - d_{13}^2 d_{24} - d_{13} d_{24}^2 - d_{23}^2 d_{14} - d_{23} d_{14}^2 \\ &\quad -d_{12} d_{13} d_{23} - d_{12} d_{14} d_{24} - d_{13} d_{14} d_{34} - d_{23} d_{24} d_{34} + d_{12} d_{13} d_{24} + d_{12} d_{13} d_{34} \\ &\quad +d_{12} d_{23} d_{14} + d_{12} d_{23} d_{34} + d_{13} d_{23} d_{14} + d_{13} d_{23} d_{24} + d_{12} d_{14} d_{34} \\ &\quad +d_{12} d_{24} d_{34} + d_{13} d_{14} d_{24} + d_{13} d_{24} d_{34} + d_{23} d_{14} d_{24} + d_{23} d_{14} d_{34}). \end{aligned}$$

Definition 2.27 *We say that d satisfies the* tetragonal inequalities *on V_4 if*

$$\begin{aligned} f_{T_1}(d) &:= 2d_{12}d_{34} - |d_{13}^2 + d_{24}^2 - d_{23}^2 - d_{14}^2| \geq 0, \quad (T_1) \\ f_{T_2}(d) &:= 2d_{14}d_{23} - |d_{12}^2 + d_{34}^2 - d_{13}^2 - d_{24}^2| \geq 0, \quad (T_2) \\ f_{T_3}(d) &:= 2d_{13}d_{24} - |d_{23}^2 + d_{14}^2 - d_{12}^2 - d_{34}^2| \geq 0. \quad (T_3) \end{aligned}$$

Theorem 2.28 *Let, for $i = 1, 2, 3$, $C_4^{\sqrt{SM},iT}$ denote the set of all $d \in C_4^{\sqrt{SM}}$ where $\sqrt{d}$ fulfills exactly i of the 3 inequlities $(T_1) - (T_3)$.*
Then we have the following chain of inclusions:

$$C_4^{\text{eucl}} \subsetneq C_4^{\sqrt{SM},3T} \subsetneq C_4^{\sqrt{SM},2T} \subsetneq C_4^{\sqrt{SM},T} = C_4^{\sqrt{SM}}.$$

Proof. - For any subset $I \subset V_n$, we construct the principal submatrix $A_I := (a_{ij})_{i,j \in I}$ of A by removing all rows and columns of A which are not in I. According to Prop. 2.24, $(X, \sqrt{d})$ is euclidean iff the matrix $A = (\text{id}_n - es^\top)(-D)(\text{id}_n - se^\top)$ is positive semidefinite for any $s \in \mathbb{R}^n$ with $s^\top e = 1$. Therefore, if $(V_n, \sqrt{d})$ is euclidean, we have $\det(A_I) \geq 0 \ \forall I \subset V_n$. Choose for example $s^\top = (0, 1, 1, -1)$ then we have

$$0 \leq \det A_{\{1,2\}} = 4d_{12}d_{34} - (d_{13} + d_{24} - d_{23} - d_{14})^2 \Leftrightarrow f_{T_1}(\sqrt{d}) \geq 0.$$

Analogously $\det A_{\{1,3\}} \geq 0$ implies (T_3), and if we set $s^\top = (0, 1, -1, 1)$, then $\det A_{\{1,4\}} \geq 0$ implies (T_2). So we have proved the inclusion $C_4^{\text{eucl}} \subset C_4^{\sqrt{SM},3T}$, while all other inclusions are trivial.
Define the distance d on V_4 by $d_{12} = d_{13} = d_{23} = 1$ and $d_{14} = d_{24} = d_{34} = 2$. Then d fulfills the triangle inequalities and $(T_1) - (T_3)$, but d is not euclidean, since $\det CM(V_4, d^2) = -2^5 < 0$, i.e., $d^2 \in C_4^{\sqrt{SM},3T}$, but $d^2 \notin C_4^{\text{eucl}}$.
Consider the semimetric space (V_4, d) defined by $d_{12} = d_{23} = 1$, $d_{13} = d_{14} = 2$ and $d_{24} = d_{34} = 3$. Then we have

$$\begin{aligned} 2d_{12}d_{34} = 2 \cdot 1 \cdot 3 = 6 \ &\not\geq\ |d_{13}^2 + d_{24}^2 - d_{23}^2 - d_{14}^2| = |2^2 + 3^2 - 1^2 - 2^2| = 8, \\ 2d_{14}d_{23} = 2 \cdot 2 \cdot 1 = 4 \ &\geq\ |d_{12}^2 + d_{34}^2 - d_{13}^2 - d_{24}^2| = |1^2 + 3^2 - 2^2 - 3^2| = 3, \\ 2d_{13}d_{24} = 2 \cdot 2 \cdot 3 = 12 \ &\geq\ |d_{23}^2 + d_{14}^2 - d_{12}^2 - d_{34}^2| = |1^2 + 2^2 - 1^2 - 3^2| = 5, \end{aligned}$$

i.e., $d^2 \in C_4^{\sqrt{SM},2T}$, but $d^2 \notin C_4^{\sqrt{SM},3T}$.
Further, the distance d on V_4 defined by $d_{12} = d_{23} = d_{34} = d_{14} = 1$ and $d_{13} = d_{24} = 2$ is an example for $d^2 \in C_4^{\sqrt{SM}}$, but $d^2 \notin C_4^{\sqrt{SM},2T}$.
Since

$$\begin{aligned} 0 &\leq \sum_{1\leq i<j<k\leq 4} (2d_{ij}d_{ik} + 2d_{ij}d_{jk} + 2d_{ik}d_{jk} - d_{ij}^2 - d_{ik}^2 - d_{jk}^2) \\ &= 4d_{12}d_{34} - (d_{13} + d_{24} - d_{23} - d_{14})^2 + 4d_{14}d_{23} - (d_{12} + d_{34} - d_{13} - d_{24})^2 \\ &\quad +4d_{13}d_{24} - (d_{23} + d_{14} - d_{12} - d_{34})^2, \end{aligned}$$

every semimetric satisfies at least one tetragonal inequality. This implies $C_4^{\sqrt{SM},T} = C_4^{\sqrt{SM}}$. □

2.3.3 Braid action on distance spaces

Consider the BKL_n^+-action on $V^* \cong \mathbb{R}^{E_n}$ already defined in the proof of corollary 2.17: $x \cdot v^* := (\rho_0^* x)v^*$.
Write $v^* = \sum_{i<j} d_{ij}v_{ij}^*$ with $d_{ij} = \langle v^* \mid v_{ij}\rangle$, and $(\rho_0^* x)v^* = \sum_{i<j} d'_{ij}v_{ij}^*$ with

$$d'_{ij} := \langle(\rho_0^* x)v^* \mid v_{ij}\rangle = \langle v^* \mid (\rho_0(\mathrm{rev}x))v_{ij}\rangle.$$

Then, for $x = a_{ts}$, we have for all i, j, k with $1 \leq i < s < j < t < k \leq n$:

$$\begin{array}{rcl} d'_{st} &=& 0, \\ d'_{is} &=& d_{is}, \quad d'_{it} \;=\; d_{is}, \\ d'_{sj} &=& t^{-1}d_{jt}, \quad d'_{jt} \;=\; d_{jt}, \\ d'_{sk} &=& d_{sk}, \quad d'_{tk} \;=\; d_{sk}, \\ d'_{ij} &=& d_{is} + d_{ij} - d_{it} - d_{sj} + d_{st} + t^{-1}d_{jt}, \\ d'_{jk} &=& -td_{sj} + td_{st} + d_{sk} + d_{jt} + d_{jk} - d_{tk}, \end{array}$$

and $d'_{i_1i_2} = d_{i_1i_2}$ for all i_1, i_2 with $\{s, t\} \cap \{i_1, i_2\} = \emptyset$.
Now let d_{ij} be $\forall i, j \in V_n$ a matrix element of a distance matrix D, i.e., v^* describes a distance. It is a natural question to ask under which circumstances does $x \cdot v^*$ ($x \in BKL_n^+$) describe a distance, too, or more precisely, on which subsets of V^* does BKL_n^+ act.
First, we consider the case $t = 1$.

Theorem 2.29 *For $t = 1$ BKL_n^+ acts on $C_n^{\mathrm{eucl}} \subset V^*$, i.e.,*

$$(BKL_n^+)C_n^{\mathrm{eucl}} \subset C_n^{\mathrm{eucl}}.$$

PROOF. - According to proposition 2.23 $v^* = \sum_{i<j} d_{ij} v^*_{ij} \in C_n^{\mathrm{eucl}}$ satisfies $\sum_{1\leq i<j\leq n} b_i b_j d_{ij} \leq 0$ for all $b \in \mathbb{Z}^n$ with $\sum_{i=1}^n b_i = 0$.
Then, for $d' := (\rho_0^* a_{ts}) v^* = \sum_{i<j} d'_{ij} v^*_{ij}$, we have

$$
\begin{aligned}
\sum_{1\leq i<j\leq n} b_i b_j d'_{ij} &= \sum_{i<s} b_i (b_s d'_{is} + b_t d'_{it}) + \sum_{s<j<t} b_j (b_s d'_{sj} + b_t d'_{jt}) \\
&\quad + \sum_{t<k} (b_s d'_{sk} + b_t d'_{tk}) b_k + \sum_{i<s<j<t} b_i b_j d'_{ij} + \sum_{s<j<t<k} b_j b_k d'_{jk} \\
&\quad + (\sum_{i_1,i_2<s} + \sum_{s<i_1,i_2<t} + \sum_{t<i_1,i_2} + \sum_{i_1<s<t<i_2}) b_{i_1} b_{i_2} d'_{i_1 i_2} \\
&= \sum_{i<s} b_i (b_s + b_t) d_{is} + \sum_{s<j<t} b_j (b_s + b_t) d_{jt} + \sum_{t<k} b_k (b_s + b_t) d_{sk} \\
&\quad + \sum_{i<s<j<t} b_i b_j (d_{is} + d_{ij} - d_{sj} - d_{it} + d_{st} + d_{jt}) \\
&\quad + \sum_{s<j<t<k} b_j b_k (-d_{sj} + d_{st} + d_{jt} + d_{sk} + d_{jk} - d_{tk}) \\
&\quad + (\sum_{i_1,i_2<s} + \sum_{s<i_1,i_2<t} + \sum_{t<i_1,i_2} + \sum_{i_1<s<t<i_2}) b_{i_1} b_{i_2} d_{i_1 i_2}.
\end{aligned}
$$

These terms can be regrouped to

$$
\begin{aligned}
Q_n(b)^\top d' &= \sum_{i<s} b_i [(b_s + \sum_{s<j<t} b_j + b_t) d_{is} + (- \sum_{s<j<t} b_j) d_{it}] \\
&\quad + \sum_{s<j<t} b_j [(-\sum_{i<s} b_i - \sum_{t<k} b_k) d_{sj} + (\sum_{i<s} b_i + b_s + b_t + \sum_{t<k} b_k) d_{jt}] \\
&\quad + \sum_{t<k} b_k [(b_s + \sum_{s<j<t} b_j + b_t) d_{sk} + (- \sum_{s<j<t} b_j) d_{tk}] \\
&\quad + (- \sum_{s<j<t} b_j)(\sum_{i<s} b_i + \sum_{t<k} b_k) d_{st} + \sum_{\{i,j\}\cap\{s,t\}=\emptyset} b_i b_j d_{ij} \overset{!}{=} \sum_{i<j} b'_i b'_j d_{ij},
\end{aligned}
$$

where $b' \in \mathbb{Z}$, defined by

$$
\begin{aligned}
b'_s &= \sum_{s\leq j\leq t} b_j = - \sum_{i<s} b_i - \sum_{t<k} b_k, \\
b'_t &= - \sum_{s<j<t} b_j = \sum_{i\leq s} b_i + \sum_{t\leq k} b_k \quad \text{and} \\
b'_i &= b_i \quad \forall i \notin \{s,t\},
\end{aligned}
$$

satisfies $\sum_{i=1}^n b'_i = 0$. Therefore we have proved $Q_n(b)^\top d' \leq 0$ for all $b \in \mathbb{Z}$ with $\sum_{i=1}^n b_i = 0$, i.e. $(\rho_0^* a_{ts}) v^* \in C_n^{\mathrm{eucl}}$.

Then $(\rho_0^* x)v^* \in C_n^{\mathrm{eucl}}$ for all $x \in BKL_n^+$ is proved by induction over $l_{Q_1}(x)$. □

But for $n = 4$, BKL_n^+ acts on other subsets of $V^* \cong \mathbb{R}^6$, too.

Theorem 2.30 *Let $C_4^{\sqrt{SM},T_1,T_2}$ denote the set of all $d \in C_4^{\sqrt{SM}}$ where d fulfills the tetragonal inequalities $(T_1), (T_2)$.*
Then, for $n = 4$ and $t = 1$, BKL_n^+ acts on $C_4^{\sqrt{SM},T_1,T_2}$ and $C_4^{\sqrt{SM},3T}$, i.e.

$$BKL_n^+ C_4^{\sqrt{SM},T_1,T_2} \subset C_4^{\sqrt{SM},T_1,T_2} \quad \text{and} \quad BKL_n^+ C_4^{\sqrt{SM},3T} \subset C_4^{\sqrt{SM},3T}.$$

Proof. - The first assertion will be proved later.
In order to prove the second assertion we have to verify

$$f_{T_3}(\sqrt{d'}) \geq 0 \quad \Leftrightarrow \quad 4d'_{13}d'_{24} - (d'_{12} + d'_{34} - d'_{14} - d'_{23})^2 \geq 0$$

with $d'_{ij} := \langle (\rho_0^* x)v^* \mid v_{ij} \rangle$ for all $1 \leq s < t \leq n$

$$f_{T_3}(d') = \begin{cases} 4d_{13}d_{14} - (0 + d_{34} - d_{14} - d_{13})^2 \geq 0, & (\Delta(1,3,4)) \quad (s,t) = (1,2), \\ 4d_{12}d_{24} - (d_{12} + d_{24} - d_{14} - 0)^2 \geq 0, & (\Delta(1,2,4)) \quad (s,t) = (2,3), \\ 4d_{13}d_{23} - (d_{12} + 0 - d_{13} - d_{23})^2 \geq 0, & (\Delta(1,2,3)) \quad (s,t) = (3,4), \\ 4d_{34}d_{24} - (d_{24} + d_{34} - 0 - d_{23})^2 \geq 0, & (\Delta(2,3,4)) \quad (s,t) = (1,4), \\ 0 - (d_{23} + d_{14} - d_{14} - d_{23})^2 = 0 \geq 0, & \checkmark \quad (s,t) = (1,3), \\ 0 - (d_{12} + d_{34} - d_{12} - d_{34})^2 = 0 \geq 0, & \checkmark \quad (s,t) = (2,4). \end{cases}$$

Here the first four inequalites are valid since $\sqrt{d}$ satisfies the triangle inequalities $\Delta(i,j,k)$ for all $1 \leq i < j < k \leq 4$. □

But in order to prove injectivity of the LK representation ρ of B_4 for $t \in (0,1)$, we have to introduce t-generalized versions of the above defined subset of V^*.
It is not known so far, whether there exists a proper notion of "t-euclidicity" for $n \geq 4$. We leave it as an open problem.
But Krammer introduced a proper t-generalization of the triangle inequalities **[Kr00]**:

Definition 2.31 *The distance space (V_n, d) is called a t-semimetric space if it fulfilles the following t-triangle inequalities*

$$\begin{array}{rcll} d_{ik} & \leq & d_{ij} + d_{j,k}, & (D_1) \\ d_{ij} & \leq & d_{ik} + t^{-1/2} d_{jk}, & (D_2) \\ d_{jk} & \leq & d_{ik} + t^{1/2} d_{ij} & (D_3) \end{array}$$

for all $1 \le i < j < k \le n$.

Since $d_{ij} \ge 0 \ \forall i < j$, we are allowed to square the inequalities $(D_1)-(D_3)$. Therefore these linear inequalities in d are obviously equivalent to

$$\begin{array}{lclcl} (D_1) & \Leftrightarrow & d_{ij}^2 - d_{ik}^2 + d_{jk}^2 & \ge & -2d_{ij}d_{jk}, \\ (D_2) & \Leftrightarrow & -td_{ij}^2 + td_{ik}^2 + d_{jk}^2 & \ge & -2pd_{ik}d_{jk}, \\ (D_3) & \Leftrightarrow & td_{ij}^2 + d_{ik}^2 - d_{jk}^2 & \ge & -2pd_{ij}d_{ik}. \end{array}$$

But there are other sufficient and/or necessary conditions for d to be a t-semimetric.

Lemma 2.32 *a) d is a t-semimetric on V_n iff it satisfies the following inequalities:*

$$\begin{array}{rcll} 2d_{ik}d_{jk} & \ge & -d_{ij}^2 + d_{ik}^2 + d_{jk}^2, & (\tilde{D}_1) \\ 2d_{ij}d_{ik} & \ge & d_{ij}^2 + d_{ik}^2 - t^{-1}d_{jk}^2, & (\tilde{D}_2) \\ 2d_{ij}d_{jk} & \ge & pd_{ij}^2 - p^{-1}d_{ik}^2 + p^{-1}d_{jk}^2. & (\tilde{D}_3) \end{array}$$

b) If (V_n, d) is a t-semimetric space, then d fulfilles the following inequalities:

$$\begin{array}{rcll} 2p^{-1}d_{ij}d_{jk} & \ge & d_{ij}^2 - d_{ik}^2 + d_{jk}^2, & (E_1) \\ 2d_{ik}d_{jk} & \ge & -td_{ij}^2 + td_{ik}^2 + d_{jk}^2, & (E_2) \\ 2d_{ij}d_{ik} & \ge & td_{ij}^2 + d_{ik}^2 - d_{jk}^2. & (E_3) \end{array}$$

Proof. - a) Since $(\tilde{D}_1)$, $(\tilde{D}_2)$, $(\tilde{D}_3)$, are equivalent to

$$d_{ij} \ge |d_{ik} - d_{jk}|, \ p^{-1}d_{jk} \ge |d_{ij} - d_{ik}|, \ d_{ik} \ge |d_{jk} - pd_{ij}|$$

respectively, it is clear that $(\tilde{D}_l) \Rightarrow (D_l)$ for $l = 1, 2, 3$.
And $(D_{l-1\,\mathrm{mod}3}) \wedge (D_l) \Rightarrow (D_l)$ for $l = 1, 2, 3$ follows from

$$-d_{ij} \overset{(D_1)}{\le} d_{jk} - d_{ik} \overset{(D_3)}{\le} pd_{ij} \le d_{ij}, \ -p^{-1}d_{jk} \le -d_{jk} \overset{(D_1)}{\le} d_{ij} - d_{ik} \overset{(D_2)}{\le} p^{-1}d_{jk},$$

$$\text{and} - d_{ik} \le -pd_{ik} \overset{(D_2)}{\le} d_{jk} - pd_{ij} \overset{(D_3)}{\le} pd_{ik} \le d_{ik}, \text{respectivly.}$$

b) Proof of (E_1): We study the cases $d_{ij} \ge p^{-1}d_{jk}$ and $p^{-1}d_{jk} \ge d_{ij}$ separately.

$$\begin{array}{rl} 1) & d_{ij} \ge p^{-1}d_{jk} \quad \Rightarrow d_{ik} \overset{(D_2)}{\ge} d_{ij} - p^{-1}d_{jk} \ge 0 \Rightarrow d_{ik}^2 \ge (d_{ij} - p^{-1}d_{jk})^2 \Rightarrow \\ & 2p^{-1}d_{ij}d_{jk} - d_{ij}^2 - d_{jk}^2 + d_{ik}^2 \ge 2p^{-1}d_{ij}d_{jk} - d_{ij}^2 - d_{jk}^2 + (d_{ij} - p^{-1}d_{jk})^2 \\ = & (t^{-1} - 1)d_{jk}^2 \ge 0 \quad \Leftrightarrow (E_1). \end{array}$$

$$\begin{array}{rl} 2) & p^{-1}d_{jk} \ge d_{ij} \quad \Rightarrow d_{ik} \overset{(D_3)}{\ge} d_{jk} - pd_{ij} \ge 0 \Rightarrow d_{ik}^2 \ge (d_{jk} - pd_{ij})^2 \Rightarrow \\ & 2p^{-1}d_{ij}d_{jk} - d_{ij}^2 - d_{jk}^2 + d_{ik}^2 \ge 2p^{-1}d_{ij}d_{jk} - d_{ij}^2 - d_{jk}^2 + (d_{jk} - pd_{ij})^2 \\ = & 2p^{-1}d_{ij}d_{jk} - d_{ij}^2 - d_{jk}^2 + td_{ij}^2 - 2pd_{ij}d_{jk} + d_{jk}^2 \\ = & (p^{-1} - p)d_{ij}d_{jk} + (1-t)d_{ij}[p^{-1}d_{jk} - d_{ij}] \overset{2)}{\ge} 0 \quad \Leftrightarrow (E_1). \end{array}$$

Proof of (E_2):

$$\begin{array}{rl}
1) & d_{jk} \geq d_{ik} \quad \Rightarrow pd_{ij} \overset{(D_3)}{\geq} d_{jk} - d_{ik} \geq 0 \Rightarrow td_{ij}^2 \geq (d_{ik} - d_{jk})^2 \Rightarrow \\
& 2d_{ik}d_{jk} - td_{ik}^2 - d_{jk}^2 + td_{ij}^2 \geq 2d_{ik}d_{jk} - td_{ik}^2 - d_{jk}^2 + (d_{ik} - d_{jk})^2 \\
= & (1-t)d_{ik}^2 \geq 0 \quad \Leftrightarrow (E_2). \\
2) & d_{ik} \geq d_{jk} \quad \Rightarrow d_{ij} \overset{(D_1)}{\geq} d_{ik} - pd_{jk} \geq 0 \Rightarrow d_{ij}^2 \geq (d_{ik} - pd_{jk})^2 \Rightarrow \\
& 2d_{ik}d_{jk} - td_{ik}^2 - d_{jk}^2 + td_{ij}^2 \geq 2d_{ik}d_{jk} - td_{ik}^2 - d_{jk}^2 + td_{ij}^2 + (d_{ik} - pd_{jk})^2 \\
= & (1-t)d_{ik}d_{jk} + (1-t)d_{jk}[d_{ik} - d_{jk}] \overset{2)}{\geq} 0 \quad \Leftrightarrow (E_2).
\end{array}$$

Proof of (E_3):

$$\begin{array}{rl}
1) & d_{ik} \geq d_{ij} \quad \Rightarrow d_{jk} \overset{(D_1)}{\geq} d_{ik} - d_{ij} \geq 0 \Rightarrow d_{jk}^2 \geq (d_{ij} - d_{ik})^2 \Rightarrow \\
& 2d_{ij}d_{ik} - td_{ij}^2 - d_{ik}^2 + d_{jk}^2 \geq 2d_{ij}d_{ik} - td_{ij}^2 - d_{ik}^2 + (d_{ij} - d_{ik})^2 \\
= & (1-t)d_{ij}^2 \geq 0 \quad \Leftrightarrow (E_3).
\end{array}$$

$$\begin{array}{rl}
2) & d_{ij} \geq d_{ik} \quad \Rightarrow d_{jk} \overset{(D_2)}{\geq} p(d_{ij} - d_{ik}) \geq 0 \Rightarrow d_{ik}^2 \geq t(d_{ij} - d_{ik})^2 \Rightarrow \\
& 2d_{ij}d_{ik} - td_{ij}^2 - d_{ik}^2 + d_{jk}^2 \geq 2d_{ij}d_{ik} - td_{ij}^2 - d_{ik}^2 + t(d_{ij} - d_{ik})^2 \\
= & (1-t)d_{ij}d_{ik} + (1-t)d_{ik}[d_{ij} - d_{ik}] \overset{2)}{\geq} 0 \quad \Leftrightarrow (E_3). \quad \square
\end{array}$$

Each t-semimetric has the the following properties:

Lemma 2.33 *Let (V_n, d) be a t-semimetric space. Then d satisfies $(1 \leq q < r < s < t \leq n)$*

$$(a) \qquad d_{st} = 0 \Rightarrow \begin{cases} d_{is} = d_{it} & \forall i < s \\ d_{sj} = p^{-1}d_{jt} & \forall s < j < t \\ d_{sk} = d_{tk} & \forall t < k \end{cases} .$$

$$(b) \qquad t \neq 1: \ d_{qs} = d_{rt} = 0 \Rightarrow d_{qr} = d_{rs} = d_{st} = d_{qt} = 0.$$

Proof. - For $d_{st} = 0$, the t-triangle inequalities $D_2(s, j, t)$ and $D_3(s, j, t)$ $(s < j < t)$ turn to

$$d_{sj} \leq p^{-1}d_{jt} \quad \text{and} \quad d_{jt} \leq pd_{sj} \Leftrightarrow d_{sj} = p^{-1}d_{jt}.$$

Analogously $D_1(i, s, t)$ and $D_3(i, s, t)$ $(i < s)$ imply $d_{is} = d_{it}$, and $D_1(s, t, k)$ and $D_2(s, t, k)$ $(t < k)$ imply $d_{sk} = d_{tk}$. This proves property (a)
According to property (a) we have $(1 \leq q < r < s < t \leq n)$

$$d_{qs} = 0 \Rightarrow \begin{cases} d_{qr} = p^{-1}d_{rs} \\ d_{qt} = d_{st} \end{cases} \quad \text{and} \quad d_{rt} = 0 \Rightarrow \begin{cases} d_{qr} = d_{qt} \\ d_{rs} = p^{-1}d_{st} \end{cases} .$$

This yields the following chain of equations,

$$d_{qt} = d_{qr} = p^{-1} d_{rs} = p^{-2} d_{st} = p^{-2} d_{qt},$$

which implies the assertion for $t \neq 1$. □

Definition 2.34 *The following inequalities on V_4*

$$\begin{array}{rcccll} 2p^{-1} d_{12} d_{34} & \overset{(T_{1a})}{\geq} & d_{13}^2 - d_{23}^2 - d_{14}^2 + d_{24}^2 & \overset{(T_{1b})}{\geq} & -2 d_{12} d_{34}, & (T_1) \\ 2 d_{23} d_{14} & \overset{(T_{2a})}{\geq} & -t d_{12}^2 + t d_{13} + d_{24} - d_{34}^2 & \overset{(T_{2b})}{\geq} & -2p d_{23} d_{14} & (T_2) \end{array}$$

*are called t-*tetragonal inequalities *for d.*

Define $\gamma_n \in Aut(V)$ and $\gamma_n^* \in Aut(V^*)$ by $\rho\delta_n = q^2 \gamma_n$ and $\rho^* \delta_n = q^2 \gamma_n^*$, respectively. Then the $\gamma^{(*)}$-action on (dual) standard fork basis elements is

$$\gamma_n v_{ij} = \left\{ \begin{array}{ll} v_{i+1,j+1}, & j < n \\ t v_{1,i+1}, & j = n \end{array} \right. \quad \text{and} \quad \gamma_n^* v_{ij}^* = \left\{ \begin{array}{ll} v_{i-1,j-1}^*, & i > 1 \\ t v_{j-1,n}^*, & i = 1 \end{array} \right. .$$

Write $v^* = \sum_{i<j} d_{ij} v_{ij}^*$ and $\gamma_n^* v^* = \sum_{i<j} \tilde{d}_{ij} v_{ij}^*$, then we have

$$\tilde{d}_{ij} = \langle \gamma_n^* v^* \mid v_{ij} \rangle = \langle v^* \mid \gamma_n v_{ij} \rangle = \left\{ \begin{array}{ll} d_{i+1,j+1}, & j < n \\ t d_{1,i+1}, & j = n \end{array} \right. .$$

Lemma 2.35 *We use the notation*

$$\begin{array}{rcl} C_n^{\sqrt{SM}}(t) & := & \{ d \in \mathbb{R}^{E_n} \mid \sqrt{d} \text{ is t-semimetric on } V_n \} \quad \text{and} \\ C_n^{\sqrt{T_1,T_2}}(t) & := & \{ d \in \mathbb{R}^{E_n} \mid \sqrt{d} \text{ is a distance and fulfills } T_1(t), T_2(t). \}. \end{array}$$

Then we have

$$\gamma_n^* C_n^{\sqrt{SM}}(t) = C_n^{\sqrt{SM}}(t) \quad \text{and} \quad \gamma_n^* C_4^{\sqrt{T_1,T_2}}(t) = C_4^{\sqrt{T_1,T_2}}(t).$$

Proof. - For $l = 1,2,3$, define $C_n^{\sqrt{D_l}}(i,j,k)$ $(1 \leq i < j < k \leq n)$ as the set of all vectors $\sum_{i<j} d_{ij} v_{ij}^*$ where $d_{ij} \geq 0$ and $\sqrt{d}$ satisfies $D_l(i,j,k)$. Then $C_n^{\sqrt{SM}}(t)$ is the intersection of all $C_n^{\sqrt{D_l}}(i,j,k)$. We will show that γ_n^* permutes the $C_n^{\sqrt{D_l}}(i,j,k)$.
Obviously we have $\gamma_n^* v^* \in C_n^{\sqrt{D_l}}(i,j,k) \Leftrightarrow v^* \in C_n^{\sqrt{D_l}}(i+1,j+1,k+1)$ for

$k < n$. In the case $k = n$ we have

$$\begin{aligned} & \gamma_n^* v^* \in C_n^{\sqrt{D_1}}(i,j,n) \Leftrightarrow \sqrt{\tilde{d}_{in}} \leq \sqrt{\tilde{d}_{ij}} + \sqrt{\tilde{d}_{jn}} \\ \Leftrightarrow \quad & p\sqrt{d_{1,i+1}} \leq \sqrt{d_{i+1,j+1}} + p\sqrt{d_{1,j+1}} \Leftrightarrow v^* \in C_n^{\sqrt{D_2}}(1, i+1, j+1), \\ & \gamma_n^* v^* \in C_n^{\sqrt{D_2}}(i,j,n) \Leftrightarrow \sqrt{\tilde{d}_{ij}} \leq \sqrt{\tilde{d}_{in}} + p^{-1}\sqrt{\tilde{d}_{jn}} \\ \Leftrightarrow \quad & \sqrt{d_{i+1,j+1}} \leq p\sqrt{d_{1,i+1}} + \sqrt{d_{1,j+1}} \Leftrightarrow v^* \in C_n^{\sqrt{D_3}}(1, i+1, j+1), \\ & \gamma_n^* v^* \in C_n^{\sqrt{D_3}}(i,j,n) \Leftrightarrow \sqrt{\tilde{d}_{jn}} \leq \sqrt{\tilde{d}_{in}} + p\sqrt{\tilde{d}_{ij}} \\ \Leftrightarrow \quad & p\sqrt{d_{1,j+1}} \leq p\sqrt{d_{1,i+1}} + p\sqrt{d_{i+1,j+1}} \Leftrightarrow v^* \in C_n^{\sqrt{D_1}}(1, i+1, j+1). \end{aligned}$$

This proves the first assertion.
Further, define $C_4^{\sqrt{T_1}}(t), C_4^{\sqrt{T_2}}(t)$ as the sets of all vectors $\sum_{i<j} d_{ij} v_{ij}^*$ with $d_{ij} \geq 0$ $(1 \leq i < j \leq 4)$ where $\sqrt{d}$ satisfies $T_1(t), T_2(t)$, respectively. Then we have $C_4^{\sqrt{T_1,T_2}}(t) = C_4^{\sqrt{T_1}}(t) \cap C_4^{\sqrt{T_2}}(t)$ and

$$\begin{aligned} \gamma_n^* v^* \in C_4^{\sqrt{T_1}}(t) \quad & \Leftrightarrow \quad 2p^{-1}\tilde{d}_{12}^{1/2}\tilde{d}_{34}^{1/2} \geq \tilde{d}_{13} - \tilde{d}_{23} - \tilde{d}_{14} + \tilde{d}_{24} \geq -2\tilde{d}_{12}^{1/2}\tilde{d}_{34}^{1/2} \\ & \Leftrightarrow \quad 2d_{23}^{1/2}d_{14}^{1/2} \geq d_{24} - d_{34} - td_{12} + td_{13} \geq -2pd_{23}^{1/2}d_{14}^{1/2} \\ & \Leftrightarrow \quad v^* \in C_4^{\sqrt{T_2}}(t) \quad \text{and} \\ \gamma_n^* v^* \in C_4^{\sqrt{T_2}}(t) \quad & \Leftrightarrow \quad 2\tilde{d}_{23}^{1/2}\tilde{d}_{14}^{1/2} \geq -t\tilde{d}_{12} + t\tilde{d}_{13} + \tilde{d}_{24} - \tilde{d}_{34} \geq -2p\tilde{d}_{23}^{1/2}\tilde{d}_{14}^{1/2} \\ & \Leftrightarrow \quad 2pd_{34}^{1/2}d_{12}^{1/2} \geq -td_{23} + td_{24} + td_{13} - td_{14} \geq -2td_{34}^{1/2}d_{12}^{1/2} \\ & \Leftrightarrow \quad v^* \in C_4^{\sqrt{T_1}}(t). \quad \square \end{aligned}$$

Theorem 2.36 *Recall the BKL_n^+-action on V^* defined by $x \cdot v^* = (\rho_0^* x)v \,\forall x \in BKL_n^+$. Then BKL_4^+ acts on $C_4(t) := C_4^{\sqrt{SM}}(t) \cap C_4^{\sqrt{T_1,T_2}}(t)$, i.e.*

$$x \cdot C_4(t) \subset C_4(t) \quad \forall x \in BKL_n^+.$$

Proof. - We prove the assertion by induction over $l_{Q_1}(x)$. Therefore we have to verify $a_{ts}C_4(t) \subset C_4(t)$ for all $1 \leq s < t \leq n$. Because of Lemma 2.35 we have $\gamma_4^* C_4(t) = C_4(t)$. Therefore $xC_4(t) \subset C_4(t)$ implies $\gamma_4^* x C_4(t) \subset \gamma_4^* C_4(t) = C_4(t)$. This is equivalent to

$$\gamma_4^* x C_4(t) = \gamma_4^*(\rho_0^* x)(\gamma_4^*)^{-1}\gamma_4^* C_4(t) = (\rho_0^* \delta_4 x \delta_4^{-1})C_4(t) \subset C_4(t).$$

Therefore it suffices to show $v'^* := a_{ts}v^* \in C_4(t)$ $\forall v^* \in C_4(t)$ just for one representant of each generator orbit (under the shift automorphism $\delta_4(\cdot)\delta_4^{-1}$). The orbits in question are $\{a_{43}, a_{32}, a_{21}, a_{41}\}$ and $\{a_{42}, a_{31}\}$, and we study the cases $(s,t) = (3,4)$ and $(s,t) = (2,4)$. Recall the notation $d'_{ij} = \langle a_{ts} \cdot v^* \mid v_{ij} \rangle$

and $d_{ij} = \langle v^* \mid v_{ij} \rangle$ with $1 \leq s < t \leq n$.

1) $(s,t) = (3,4)$: Since $v'^* \in \mathrm{im}(\rho_0^* a_{43})$ we have $d'_{34} = 0, d'_{13} = d'_{14}$ and $d'_{23} = d'_{24}$. This allows us to express all t-triangle inequalities (for $\sqrt{d'}$) in terms of $d'_{12}, d'_{13}, d'_{23}$. So we have just to verify the 3 inequalities $D_l(1,2,3)$ $(l = 1,2,3)$ for $\sqrt{d'}$ instead of all 12 t-triangle inequalities $D_l(i,j,k)$ $(l = 1,2,3$ and $1 \leq i < j < k \leq 4)$. But, since $d'_{12} = d_{12}, d'_{13} = d_{13}$ and $d'_{23} = d_{23}$, we have $d_{ij} \geq 0 \Rightarrow d'_{ij} \geq 0 \ \forall i < j$ and $\sqrt{d'}$ fulfilles these inequalities if $\sqrt{d}$ does.

It remains to verify the t-tetragonal inequalities for $\sqrt{d'}$.

$$\begin{array}{rcl}
(T_{1a}): & & 2p^{-1} d'^{1/2}_{12} d'^{1/2}_{34} - (d'_{13} - d'_{23} - d'_{14} + d'_{24}) \\
& = & 0 - (d_{13} - d_{23} - d_{13} + d_{23}) = 0 \geq 0, \\
(T_{1b}): & & 2 d'^{1/2}_{12} d'^{1/2}_{34} + (d'_{13} - d'_{23} - d'_{14} + d'_{24}) \\
& = & 0 + (d_{13} - d_{23} - d_{13} + d_{23}) = 0 \geq 0, \\
(T_{2a}): & & 2 d'^{1/2}_{23} d'^{1/2}_{14} - (-t d'_{12} + t d'_{13} + d'_{24} - d'_{34}) \\
& = & 2 d^{1/2}_{23} d^{1/2}_{13} - (-t d_{12} + t d_{13} + d_{23} - 0) \overset{(E2)}{\geq} 0, \\
(T_{2b}): & & 2p d'^{1/2}_{23} d'^{1/2}_{14} + (-t d'_{12} + t d'_{13} + d'_{24} - d'_{34}) \\
& = & 2 d^{1/2}_{23} d^{1/2}_{13} + (-t d_{12} + t d_{13} + d_{23} - 0) \overset{(D2)}{\geq} 0.
\end{array}$$

2) $(s,t) = (2,4)$: First we establish that d' is a distance, i.e., $d'_{ij} \geq 0 \ \forall i < j$. The only nontrivial case is

$$d'_{13} = d_{12} + d_{13} - d_{23} - d_{14} + d_{24} + t^{-1} d_{34} \overset{(T_{1b})}{\geq} (t^{-1} - 1) d_{34} + (d^{1/2}_{12} - d^{1/2}_{34})^2 \geq 0.$$

Further, here $v'^* \in \mathrm{im}(\rho_0^* a_{42})$ implies $d'_{24} = 0, d'_{12} = d'_{14}$ and $d'_{23} = t^{-1} d'_{34}$. We express the t-triangle inequalities $D_l(i,j,k)$ (for $\sqrt{d'}$) in terms of $d'_{12}, d'_{13}, d'_{23}$. The cases $(i,j,k) = (1,2,4)$ and $(2,3,4)$ lead to trivial inequalities. The remaining cases are

$$\begin{array}{lrcl lrcl}
D_1(1,2,3): & d'^{1/2}_{13} & \leq & d'^{1/2}_{12} + d'^{1/2}_{23}, & D_1(1,3,4): & d'^{1/2}_{12} & \leq & d'^{1/2}_{13} + p d'^{1/2}_{23}, \\
D_2(1,2,3): & d'^{1/2}_{12} & \leq & d'^{1/2}_{13} + p^{-1} d'^{1/2}_{23}, & D_2(1,3,4): & d'^{1/2}_{13} & \leq & d'^{1/2}_{12} + d'^{1/2}_{23}, \\
D_3(1,2,3): & d'^{1/2}_{23} & \leq & d'^{1/2}_{13} + p d'^{1/2}_{12}, & D_3(1,3,4): & p d'^{1/2}_{23} & \leq & d'^{1/2}_{12} + p d'^{1/2}_{13}.
\end{array}$$

Therefore we have to establish the inequalities

$$\begin{array}{rcll}
d'^{1/2}_{13} & \leq & d'^{1/2}_{12} + d'^{1/2}_{23}, & (F_1) \\
d'^{1/2}_{12} & \leq & d'^{1/2}_{13} + p d'^{1/2}_{23}, & (F_2) \\
d'^{1/2}_{23} & \leq & d'^{1/2}_{13} + p d'^{1/2}_{12}, & (F_3)
\end{array}$$

which are symmetric in d'_{12}, d'_{23}.
Squaring (F_1) leads to $d'_{13} \leq d'_{12} + 2d'^{1/2}_{12} d'^{1/2}_{23} + d'_{23}$. Since

$$-d'^{1/2}_{13} \overset{(F_2)}{\leq} pd'^{1/2}_{23} - d'^{1/2}_{12} \leq d'^{1/2}_{23} - pd'^{1/2}_{12} \overset{(F_3)}{\leq} d'^{1/2}_{13},$$

we have

$$(F_2) \wedge (F_3) \quad \Leftrightarrow \quad \begin{cases} 2d'^{1/2}_{12} d'^{1/2}_{23} \geq p^{-1} d'_{12} - p^{-1} d'_{13} + pd'_{23} & (\tilde{F}_2) \\ 2d'^{1/2}_{12} d'^{1/2}_{23} \geq pd'_{12} - p^{-1} d'_{13} + p^{-1} d'_{23} & (\tilde{F}_3) \end{cases} .$$

Now $(F_1), (\tilde{F}_2)$ and $(\tilde{F}_3)$ are satisfied because of

$$\begin{array}{rl}
(F_1): & d'_{12} + 2d'^{1/2}_{12} d'^{1/2}_{23} + d'_{23} - d'_{13} \\
= & d_{12} + 2p^{-1} d^{1/2}_{12} d^{1/2}_{34} + t^{-1} d_{34} - (d_{12} + d_{13} - d_{23} - d_{14} + d_{24} + t^{-1} d_{34}) \\
= & 2p^{-1} d^{1/2}_{12} d^{1/2}_{34} - (d_{13} - d_{23} - d_{14} + d_{24}) \overset{(T_{1a})}{\geq} 0, \\
(\tilde{F}_2): & 2pd'^{1/2}_{12} d'^{1/2}_{23} - d'_{12} + d'_{13} - td'_{23} \\
= & 2d^{1/2}_{12} d^{1/2}_{34} - d_{12} + (d_{12} + d_{13} - d_{23} - d_{14} + d_{24} + t^{-1} d_{34}) - d_{34} \\
= & (t^{-1} - 1) d_{34} + 2d^{1/2}_{12} d^{1/2}_{34} + (d_{13} - d_{23} - d_{14} + d_{24}) \\
\geq & 2d^{1/2}_{12} d^{1/2}_{34} + (d_{13} - d_{23} - d_{14} + d_{24}) \overset{(T_{1b})}{\geq} 0, \\
(\tilde{F}_3): & 2pd'^{1/2}_{12} d'^{1/2}_{23} - td'_{12} + d'_{13} - d'_{23} \\
= & 2d^{1/2}_{12} d^{1/2}_{34} - td_{12} + (d_{12} + d_{13} - d_{23} - d_{14} + d_{24} + t^{-1} d_{34}) - t^{-1} d_{34} \\
= & (1 - t) d_{12} + 2d^{1/2}_{12} d^{1/2}_{34} + (d_{13} - d_{23} - d_{14} + d_{24}) \\
\geq & 2d^{1/2}_{12} d^{1/2}_{34} + (d_{13} - d_{23} - d_{14} + d_{24}) \overset{(T_{1b})}{\geq} 0.
\end{array}$$

Finally we verify the t-tetragonal inequalities for $\sqrt{d'}$:

$$\begin{array}{rl}
(T_{1a}): & 2p^{-1} d'^{1/2}_{12} d'^{1/2}_{34} - (d'_{13} - d'_{23} - d'_{14} + d'_{24}) \\
= & 2p^{-1} d^{1/2}_{12} d^{1/2}_{34} - (d_{13} - d_{23} - d_{13} + d_{23}) \overset{(T_{1a})}{\geq} 0, \\
(T_{1b}): & 2d'^{1/2}_{12} d'^{1/2}_{34} + (d'_{13} - d'_{23} - d'_{14} + d'_{24}) \\
= & 2d^{1/2}_{12} d^{1/2}_{34} + (d_{13} - d_{23} - d_{13} + d_{23}) \overset{(T_{1b})}{\geq} 0, \\
(T_{2a}): & 2d'^{1/2}_{23} d'^{1/2}_{14} - (-td'_{12} + td'_{13} + d'_{24} - d'_{34}) \\
= & 2p^{-1} d^{1/2}_{34} d^{1/2}_{12} - (-td_{12} + t(d_{12} + d_{13} - d_{23} - d_{14} + d_{24} + t^{-1} d_{34}) - d_{34}) \\
= & 2p^{-1} d^{1/2}_{12} d^{1/2}_{34} - t(d_{13} - d_{23} - d_{14} + d_{24}) \\
\geq & 2p^{-1} d^{1/2}_{12} d^{1/2}_{34} - (d_{13} - d_{23} - d_{14} + d_{24}) \overset{(T_{1a})}{\geq} 0, \\
(T_{2b}): & 2pd'^{1/2}_{23} d'^{1/2}_{14} + (-td'_{12} + td'_{13} + d'_{24} - d'_{34}) \\
= & 2d^{1/2}_{34} d^{1/2}_{12} + t(d_{13} - d_{23} - d_{14} + d_{24}) \\
\geq & 2td^{1/2}_{12} d^{1/2}_{34} + t(d_{13} - d_{23} - d_{14} + d_{24}) \overset{(T_{1b})}{\geq} 0. \quad \Box
\end{array}$$

Lemma 2.37 *The pairwise disjoint, nonempty sets*

$$D_y := \{v^* = \sum_{1\le i<j\le n} d_{ij}v^*_{ij} \in \mathrm{im}(\rho^*_0 x) \mid \forall s<t : d_{st} \ge 0 \ \wedge \ d_{st} = 0 \Leftrightarrow a_{ts} \prec y\},$$

$y \in Q$, satisfy the following properties:

(1) $\gamma^*_n D_y = D_{\delta_n y \delta_n^{-1}}$ *for all* $y \in Q$.
(2) *If* $n = 4$ *then* $xD_y \subset D_x$ *holds for all leftgreedy pairs* $(x, y) \in (Q \setminus \{a_{31}, a_{42}\}) \times Q$.

Proof. - Proof of (1).

$$\begin{aligned} & \gamma^*_n v^* = \textstyle\sum_{i<j} \tilde{d}_{ij} v^*_{ij} \in D_{\delta_n y \delta_n^{-1}} \\ \Leftrightarrow\ & (\tilde{d}_{st} = 0 \quad \Leftrightarrow \quad a_{ts} \prec \delta_n y \delta_n^{-1} \ \forall s<t) \\ \Leftrightarrow\ & (d_{s+1,t+1 \mathrm{mod} n} = 0 \quad \Leftrightarrow \quad \delta_n^{-1} a_{ts} \delta_n = a_{t+1,s+1 \mathrm{mod} n} \prec y \ \forall s<t) \\ \Leftrightarrow\ & (d_{st} = 0 \quad \Leftrightarrow \quad a_{ts} \prec y \ \forall s<t) \Leftrightarrow v^* \in D_x. \quad \square \end{aligned}$$

Evidently, we have $x \cdot \mathrm{im}(\rho^*_0 y) \subset \mathrm{im}(\rho^*_0 x)$ for all leftgreedy $(x, y) \in Q^2$. Nevertheless it is a straightforward but lengthy task to verify $xD_y \subset D_x$ for all leftgreedy $(x, y) \in (Q \setminus \{a_{31}, a_{42}\}) \times Q$ for $n = 4$. We leave it to the reader. The reader has to perform a case study as in the proof of lemma 6.5 in [**Kr00**]. The proof can be abbreviated using property (1). Note that for $x \in Q \setminus \{a_{31}, a_{42}\}$ the matrices $\rho^*_0 x$ contain just nonnegative entries. Indeed every row of these matrices contains at most one positive entry. □

Theorem 2.38 *The Lawrence-Krammer representation $\rho : B_n \to GL(\binom{n}{2}, R)$ is faithful for $n = 4$ and $t \in (0, 1)$.*

Proof. - We define pairwise disjoint, nonempty subsets $C_y := D_y \cap C_4(t)$ $(y \in Q)$ of $\mathrm{im}(\rho^*_0 y)$ and $C_4(t)$, and we will show that they fulfill the inclusion $xC_y := (\rho^*_0 x)C_y \subset C_x$ for all leftgreedy pairs $(x, y) \in Q^2$. This implies the inclusion for all $(x, y) \in BKL^+_4 \times Q$, and hence, by Lemma 2.18, we have proved the faithfulness of ρ^* (and ρ).
Using lemma 2.37 (2), we obtain for all leftgreedy $(x, y) \in (Q \setminus \{a_{31}, a_{42}\}) \times Q$

$$xC_y = x(D_y \cap C_4(t)) \subset xD_y \cap xC_4(t) \subset D_x \cap C_4(t) = C_x.$$

The orbits (under shift conjugation) of the remaining leftgreedy pairs are

$$\{(a_{42}, a_{31}), (a_{31}, a_{42})\}, \quad \{(a_{42}, a_{41}), (a_{31}, a_{43}), (a_{42}, a_{32}), (a_{31}, a_{21})\},$$
$$\{(a_{42}, a_{42}), (a_{31}, a_{31})\}, \quad \{(a_{42}, a_{41}a_{32}), (a_{31}, a_{43}a_{21})\}, \quad \{(a_{42}, e), (a_{31}, e)\}.$$

Since $C_y, C_{\delta_n y \delta_n^{-1}} \in C_4(t)$ and γ_n^* preserves $C_4(t)$, lemma 2.37 (1) implies $\gamma_n^* C_y = C_{\delta_n y \delta_n^{-1}}$ for all $y \in Q$. Now, $xC_y \subset C_x$ implies

$$\delta_n x \delta_n^{-1} C_{\delta_n x \delta_n^{-1}} = \gamma_n^*(\rho_0^* x)(\gamma_n^*)^{-1}\gamma_n^* C_y = \gamma_n^*(\rho_0^* x) C_y \subset \gamma_n^* C_x = C_{\delta_n x \delta_n^{-1}}.$$

Therefore, it suffices to show that $v^* = \sum_{i<j} d_{ij} v_{ij}^* \in C_y$ for $y = e$, a_{41}, a_{42}, a_{31}, $a_{41}a_{32}$ implies $a_{42}v^* = \sum_{i<j} d'_{ij} v_{ij}^* \in C_{a_{42}}$.
Theorem 2.36 yields $a_{42}v^* \in C(t)$. Further, we have $d'_{24} = 0$ and $d'_{12} = d'_{14} = d_{12}, td'_{23} = d'_{34} = d_{34}$. Since $d_{12}, d_{34} > 0$ for all $v^* \in C_e, C_{a_{41}}, C_{a_{42}}, C_{a_{31}}, C_{a_{41}a_{32}}$, we get $d'_{12} = d'_{14} > 0, d'_{23} > 0$ and $d'_{34} > 0$. Finally, we have

$$d'_{13} = d_{12} + d_{13} - d_{23} - d_{14} + d_{24} + t^{-1} d_{34} \overset{(T_{1b})}{\geq} (t^{-1} - 1) d_{34} + (d_{12}^{1/2} - d_{34}^{1/2})^2 \overset{(*)}{>} 0$$

because of $d_{34} > 0$. So we have proved $a_{42}C_y \subset C_{a_{42}}$ for all leftgreedy (a_{42}, y), and the proof is finished. □
Note that step $(*)$ is the argument which fails for $t = 1$.

2.4 Inverting algorithms

According to Krammers faithfulness proof of the LK representation [**Kr02**] it is possible to compute the preimage braid $x \in B_n$ of a given LK matrix ρx directly in the Garside normal form (of the Artin presentation). An explicit algorithm for inverting the LK representation was first published by Cheon and Jun in [**CJ03a**, **CJ03b**].
Recall the notation from section 2.2.

Algorithm 2.1: Invert the Lawrence Krammer representation.

```
Input: A LK matrix $\rho' x := \rho x|_{q=1/2} \in GL(\binom{n}{2}, \mathbb{Q}[t^{\pm 1}])$ in $x$-basis.
Output: The unique preimage braid $x \in B_n$ in left normal form.
Compute the smallest $p \in \mathbb{Z}$ such that $M = (\rho' \Delta_n)^p \rho' x \in GL(\binom{n}{2}, \mathbb{Q}[t])$.
Initialize $k = 0$;
while $M \neq \mathrm{Id}_V$ do
    $k := k + 1$;
    Determine the zero rows of $M|_{t=0}$, i.e., $A := x'\emptyset \subset \mathrm{Trp}$ for $M = \rho' x'$.
    Compute $x[k] := GB(A)$.
    $M := (\rho' x[k])^{-1} \cdot M$;
end while;
return LNF $x = \Delta_n^{-p} x[1] \cdots x[k]$;
```

Krammers faithfulness proof of the LK representation of B_4 [**Kr00**] given in standard fork basis can also be used to develop an inversion algorithm.

Though this inversion algorithm was not explicitly published so far, its idea is contained in the definition of the cones C_x used by Krammer in [**Kr00**]. Recall that, according to corollary 3.7 in [**BKL98**], the starting (and the finishing) set of a descending cycle $\delta_\pi = a_{t_m,t_{m-1}} a_{t_{m-1},t_{m-2}} \cdots a_{t_2,t_1}$ ($\pi = (t_m, t_{m-1}, \ldots, t_1)$ with $1 \leq t_1 < \cdots < t_m \leq n$) is given by

$$S(\delta_\pi) = F(\delta_\pi) = \{a_{t_j,t_i} \mid 1 \leq i < j \leq m\}.$$

A simple element s of the Garside monoid BKL_n^+ is given by a product of parallel descending cycles $\pi_1, \ldots, \pi_k$, i.e., $s = \pi_1 \cdots \pi_k$. And the starting (and finishing) sets of s are

$$S(s) = F(s) = S(\delta_{\pi_1}) \cup \cdots \cup S(\delta_{\pi_k}).$$

Obviously, there exists a simply computable bijection between the set of simples $S \subset BKL_n^+$ and the set of starting sets of simples. We will use this fact in the following algorithm.

Algorithm 2.2: Invert the Lawrence Krammer representation.

```
Input: A LK matrix $\rho' x := \rho x|_{t=1/2} \in GL(\binom{n}{2}, \mathbb{Q}[q^{\pm 1}])$ in sf basis.
Output: The unique preimage braid $x \in B_n$ in left normal form.
Transpose the instance matrix to obtain $\rho'^* x$.
Compute the smallest $p \in \mathbb{Z}$ such that
$M = (\rho'^* \delta_n)^p \rho'^* x \in GL(\binom{n}{2}, \mathbb{Q}[q])$.
Initialize $k = 0$;
while $M \neq \mathrm{Id}_{V^*}$ do
   $k := k + 1$;
   Compute the zero rows of $M|_{q=0}$.
   They determine a starting set $S(s)$ for some $s \in S$.
   Compute the canonical factor $s$ from $S(s)$, and set $x[k] := s$.
   $M := (\rho'^* x[k])^{-1} \cdot M$;
end while;
return LNF $x = \delta_n^{-p} x[1] \cdots x[k]$;
```

Due to the lack of a faithfulness proof of the LK representation if we set $t \in (0, 1)$, algorithm 2.2 is just a heuristic for $n \geq 5$. Nevertheless, we have implemented this algorithm using MAGMA 2.10 [**Co03**], and we have shown in thousands of computer experiments with different parameter values that the preimage braids can be recovered by algorithm 2.2 for $n \geq 5$, too. This confirms Krammers main conjecture in [**Kr00**].

Chapter 3

Computing preimage braids for the Burau representation

Recall the Burau representation $\beta : B_n \to GL(n, \mathbb{Z}[q^{\pm 1}])$ defined by

$$\beta(\sigma_i) = \mathrm{Id}_{i-1} \oplus \begin{pmatrix} 1-q & q \\ 1 & 0 \end{pmatrix} \oplus \mathrm{Id}_{n-i-1} \quad \forall i = 1, \ldots, n-1.$$

This representation is not faithful for $n \geq 5$. Since the structure of the kernel of the Burau representation is not understood so far, there exists no deterministic inversion algorithm for the Burau representation as for the Lawrence-Krammer representation. Only heuristic algorithms for computing preimage braids for the Burau representation have been developed so far. Since, for $x \in B_n$, $x' := \Delta_n^u x \in B_n^+$ for some sufficiently great $u \in \mathbb{Z}$, we may deal only with positive instance braids for the inversion heuristics. Note that u is an upper bound for $-\inf(x)$.

3.1 Hughes' algorithm

The first heuristic inversion algorithm for the Burau representation was proposed in [**Hu02**] by J. Hughes. The goal is to compute a braid $x \in B_n^+$ with $\beta(x) = X$ for a given Burau matrix $X \in \beta(B_n^+)$. Hughes' algorithm reconstructs x from $\beta(x)$ gnerator by generator from right to left. It uses the observation that, if $c_H(\beta(x))$ denotes the first column with highest q-degree entry in $\beta(x)$, then $c_H(x)$ is with high probability an element in the finishing set $F(x) := \{i \in \mathbb{Z} \mid \sigma_i \prec x\}$, at least for sufficiently short $x \in B_n^+$.

Algorithm 3.1: Hughes' Algorithm

Input: $X \in \beta(B_n^+)$.

Output: $z \in B_n^+$.

```
Compute $l$ such that $\det(X) = (-q)^l$.
$z := e$;
for $i := l$ to 1 by -1 do
    Compute $j_c := c_H(X)$.
    if $j_c = n$ then break; end if;
    $z := \sigma_{j_c} \cdot z$;
    $X := X \cdot \beta(\sigma_{j_c})^{-1}$;
end for;
return $z$;
```

Note that, since the row sum of every Burau matrix equals 1, $c_H(X) = n$ implies $X \notin \beta(B_n^+)$.

E. Lee and Park introduced a slight variation of Hughes' algorithm, which uses the fact that, if $\sigma_j \in F(x)$, then every entry in the $(j+1)$-th column of $\beta(x)$ is always in $q\mathbb{Z}[q]$ [**LP03**]. Now, let $c_{LP}(X)$ denote the integer indicating the first column containing a highest-degree entry in X among the columns whose next column's entries are all in $q\mathbb{Z}[q]$, if such a $c_{LP}(X)$ exists.

Algorithm 3.2: Lee-Park's Algorithm without self-correction

Input: $X \in \beta(B_n^+)$.

Output: $z \in B_n^+$.

```
Compute $l$ such that $\det(X) = (-q)^l$.
$z := e$;
for $i := l$ to 1 by -1 do
    if there does not exist such a $c_{LP}(X)$ then
        break;
    else
        Compute $j_c := c_{LP}(X)$.
        $z := \sigma_{j_c} \cdot z$;
        $X := X \cdot \beta(\sigma_{j_c})^{-1}$;
    end if;
end for;
return $z$;
```

We tried to reproduce the results of the computer experiments in [**LP03**]: The experiment was performed on a computer with a Mobile Intel Pentium 4 Processor 3.06 GHz and 512 MB DDR-RAM using quite comfortable implementations in MAGMA V2.10.

The tables 3.1 and 3.2 show the experimental results for the algorithms 3.1 and 3.2. On input (n, l), the program chooses at random 10000 x's from B_n^+ with $|x| = l$, computes $\rho_B(x)$ from x, computes z from $\rho_B(x)$ by each algorithm, and then checks whether or not z is equal to x by comparing their normal forms.

TABLE 3.1 Success rate of recovering x from $\beta(x)$ (unit: %)

n	5			7			10		
$\|x\|$	30	40	50	40	55	70	60	80	100
Alg. 3.1	90.89	81.36	70.61	88.71	73.72	56.71	84.74	67.74	49.94
Alg. 3.2	91.57	81.52	71.12	89.08	74.06	56.56	84.16	67.37	50.22
[**LP03**]:	96	83	76	91	76	64	87	67	42

Observation: We can reproduce similar results for the success rates of algorithm 3.2 (and algorithm 3.1) as in [**LP03**].

TABLE 3.2 Elapsed time in recovering x from $\beta(x)$ (unit: millisecond)

[t_H :=time(algorithm 3.1) and t_{LP} :=time(algorithm 3.2)]

$(n, \|x\|)$	(7,40)	(7,55)	(7,70)	(10,60)	(10,80)	(10,100)
t_H	7.1064	10.2109	13.1468	19.0047	25.8394	32.0566
t_{LP}	10.5127	14.8576	18.6722	28.1155	38.1345	46.1931
t_{LP}/t_H	1.479	1.455	1.420	1.479	1.476	1.441

(Note that this table only compares the inverting processes themselves. The time commonly taken in computing $|x|$ from $\beta(x)$ is not included.)

Observation: The measured elapsed times t_H and t_{LP} depend on the implementations. But the quotient t_{LP}/t_H decreases for increasing wordlength l (n =const.) in our experiment as in [**LP03**].

The lucid analysis in section 4.2 of [**LP03**] explains why the Hughes heuristic works so surprisingly good. Note that in the case $n = 3$ the success rate of the Hughes algorithm is 100% and the just mentioned analysis [**LP03**] contains a fatihfulness proof of the Burau representation.

3.2 Self-correcting algorithm

In [**LP03**] E. Lee and Park introduced an upgraded, self-correcting version of algorithm 3.2.

For $x \in B_n^+$, we introduce the abbreviations $x_1 = \sigma_{c_{LP}(x)}$, $x_2 = \sigma_{c_{LP}(xx_1^{-1})}$,

…, $x_k = \sigma_{c_{LP}(xx_1^{-1}\cdots x_{k-1}^{-1})}$, and $x' = xx_1^{-1}\cdots x_k^{-1}$ for $1 \leq k < |x|$. E. Lee and Park made the observation that, if $c_H(x') \neq c_{LP}(x')$, then $c_{LP}(y) \notin F(y)$ ($y := x'x_k \cdots x_i$) for some $1 \leq i \leq k$. Further they observed that, if $c_{LP}(y) > 1$ and if every entry in the $c_{LP}(y)$-th column of $\beta(y)$ is in $q\mathbb{Z}[q]$, then it is probable that $c_{LP}(y) - 1 \in F(y)$. This is the main idea of the selfcorrection in algorithm 3.3.
Here we reprint a corrected version of algorithm 2 in **[LP03]**, published as algorithm 4 in **[Le06]**. M_j denotes the j-th column of the matrix M.

Algorithm 3.3: Lee-Park's Algorithm with self-correction

```
Input: $X \in \beta(B_n^+)$.
Output: $z \in B_n^+$.
if $X = \mathrm{Id}_n$ then
    $z := e$;
else
    Compute $l$ such that $\det(X) = (-q)^l$.
    $M[l] := X$;
    for $i := l$ to 1 by -1 do
        Compute $j_a := c_H(M[i])$ and $j_c := c_{LP}(M[i])$.
        if there exists such $j_c$ and $j_c = j_a$ then
            $A[i] := j_c$; $M[i-1] := M[i] \cdot \beta(\sigma_{j_{A[i]}})^{-1}$;
        else
            if $i = l$ then
                break;
            end if;
            if there exists $k$ $(> i)$ such that $j_c = j_a > 1$ for $M[k]$,
            $A[k] = j_a$ and every entry of $M[k]_{j_c}$ is in $t\mathbb{Z}[t]$ then
                reset $i$ to be the smallest value among such $k$'s;
                $i := k$; $A[i] := A[i] - 1$; $M[i-1] := M[i] \cdot \beta(\sigma_{A[i]})^{-1}$;
            else
                break;
            end if;
        end if;
    end for;
    if $i = l$ then
        $z := e$;
    else
        $z := \sigma_{A[i]} \cdots \sigma_{A[l]}$;
    end if;
end if;
return $z$;
```

Note that in line 10 of algorithm 2 in [**LP03**], which corresponds to line 14 of algorithm 3.3, the additional condition $A[k] = j_a$ is missing, i.e., we have line

```
14_old:  if there exists $k$ ($> i$) such that $j_c = j_a > 1$ for $M[k]$
         and every entry of $M[k]_{j_c}$ is in $t\mathbb{Z}[t]$ then
```

instead of line 14. Unfortunately, this leads to the phenomenon that the selfcorrecting procedure does not work accurately, because after some "selfcorrection jumps" (line 15 in alg. 3.3) the difference between $j_a = \mathsf{C_H}(M[k])$ and $A[k]$ could become greater than 1.

Further, in line 11 of algorithm 2 in [**LP03**] the authors simply reset i to be k, without declaring which k do they choose. Of course, it is the most natural choice to select the minimal k (with the properties described in line 14 of algorithm 3.3). Indeed, this choice is made in line 15 of algorithm 3.3 (algorithm 4 in [**Le06**]).

We tried to reproduce the results for the success rates of the selfcorrecting algorithm 3.3 given in [**LP03**, **Le06**]:

We implemented algorithm 3.3 using the computer algebra system MAGMA 2.10. Now, our program only chooses at random 1000 x's from B_n^+. We also perfomed some tests to show what happens, if we choose the maximal k instead of the minimal in line 15.

TABLE 3.3 Success rate of recovering x from $\beta(x)$ using algorithm 3.3

n	5			7			10		
$\|x\|$	30	40	50	40	55	70	60	80	100
Line 14_{old}, min. k	92.8			90.3			84.5		
Line 14, min. k	99.9	99.2	99.4	99.7	98.8	98.2	99.2	98.7	96.9*
[**LP03**, **Le06**]	100	99	97	99	97	82	99	90	69
Line 14, max. k	93.3			89.2			86.4		

*We used a conditional statement (if elapsed time greater than 1 hour then break;) to reduce the expenditure of time. In so far 969 is just a lower bound for the number of successfully recoverable preimage braids in this computer experiment.

Observation: The success rates of our implementation of algorithm 3.3 are actually higher than those reported in [**LP03**]. Especially for the parameter values $(n, l) = (7, 70), (10, 80)$ and (10,100) there is a significant gap between the results in [**LP03**, **Le06**] and our results[1].

[1] We assume that E. Lee and Park used such a conditional statement as we did for the parameter value $(n, l) = (10, 100)$. Otherwise we estimate their computer experiments

3.3 An improved linear complexity algorithm

First, for the purpose of motivation, we describe an inversion algorithm for the representations $s^{-1}(\beta_s^{\mathrm{red}})^+$, $s^{-1}(\beta_s^{\mathrm{red}})^\ddagger : B_n \to GL(n^2, \mathbb{Z}[s^{\pm 1}, q^{\pm 1}])$. (See the notation used in section 1.5.)
Here the rows (and columns) of an n^2-dimensional matrix are indexed by $(i,j) \in \{1, \ldots, n\}^2$. Explicitly, the (i,j)-th row (column) of the matrix M is denoted by ${}_{(i,j)}M$ $(M_{(i,j)})$.

Algorithm 3.4: Inverting algorithm for $s^{-1}(\beta_s^{\mathrm{red}})^+$, $s^{-1}(\beta_s^{\mathrm{red}})^\ddagger$

Input: A matrix $X = \rho x$ with $\rho = s^{-1}(\beta_s^{\mathrm{red}})^+$ or $\rho = s^{-1}(\beta_s^{\mathrm{red}})^\ddagger$ for some unknown $x \in B_n$.

Output: $z \in B_n$ in right normal form.

```
Compute the smallest $p \in \mathbb{Z}$ such that
$M = \rho x(\rho\delta_n)^p \in GL(n^2, \mathbb{Z}[s, q^{\pm 1}])$.
Initialize $k := 0$;
while $M \neq \mathrm{Id}_{n^2}$ do
   $k := k + 1$;
   $St := \emptyset$;
   for $i := 1$ to $n - 1$ do
      for $j := i + 1$ to $n$ do
         if $M_{(i,k)} = M_{(j,k)}$ for all $k = 1, \ldots, n$ then
            Include $a_{ji}$ in $St$.
         end if;
      end for;
   end for;
   if $St$ is the starting set of some $\bar{s} \in Q$ then
      Compute $x[k] = \bar{s} \in Q$ such that $St = S(\bar{s})$.
   else break;
   end if;
   $M := M \cdot (\rho\bar{s})^{-1}$;
end while;
return $z = x[k] \cdots x[1]\delta_n^{-p}$;
```

This algorithm is reminiscent of algorithm 2.2 based on the ideas of D. Krammer, used in his faithfulness proof of B_4 [**Kr00**]. Obviously it has linear time complexity in the dual canonical length.
Though we are not able to prove that algorithm 3.4 computes the unique

would have taken at least a month. Keep in mind that one hour in our implementation corresponds to ca. one day in the implementation of Lee, Park. This rough estimation is deduced from the elapsed times given for the Hughes algorithm. If this assumption is true, this could explain the gap. Otherwise we have no explanation for the gap.

preimage braid $x \in B_n$ such that $X = \rho x$ ($\rho = s^{-1}(\beta_s^{\text{red}})^+$ or $\rho = s^{-1}(\beta_s^{\text{red}})^\ddagger$), hundreds of computer experiments with different parameter values, where the input braids were always reconstructed successfully, supports this assumption.

Analogously, we can apply this algorithm to the $n(n+1)$-dimensional representations $s^{-1}\beta_s^+$, $s^{-1}(\rho_s^{TYM})^+$ where ρ^{TYM} denotes the Tong-Yang-Ma representation defined by $\sigma_i \mapsto \mathrm{Id}_{i-1} \oplus \left(\begin{smallmatrix} 0 & q \\ 1 & 0 \end{smallmatrix}\right) \oplus \mathrm{Id}_{n-i-1}$. Note that in the case of $s^{-1}(\rho_s^{TYM})^+$ an analogue of algorithm 3.4 fails to recover a preimage braid with increasing probabilty for increasing length of the input braid. Indeed, we conjecture that the augmented representation $s^{-1}(\rho_s^{TYM})^+$ is not faithful for $n \geq 4$.

Further, we can apply an analogue of algorithm 3.4 to the n-dimensional representation $s^{-1}\tau_s^+$ (see example 2.(a) in section 1.5), i.e., to Burau-type representations. However, if we want to apply it to the Burau matrices, explicitly defined in section 1.2, we set $s^2 = q$ and we build a somehow reverse (or transposed) algorithm:

Algorithm 3.5: Linear inversion heuristic for the Burau represention

```
Input: A Burau matrix $X \in \beta(B_n)$.
Output: $z \in B_n$ in left normal form.
Compute the smallest $p \in \mathbb{Z}$ such that
$M = \beta x(\beta\delta_n)^p \in GL(n, \mathbb{Z}[q])$.
Initialize $k := 0$;
while $M \neq \mathrm{Id}_n$ do
    $k := k + 1$;
    $St := \emptyset$;
    for $i := 1$ to $n - 1$ do
        for $j := i + 1$ to $n$ do
            if ${}_iM =_j M$ then
                Include $a_{ji}$ in $St$.
            end if;
        end for;
    end for;
    if $St$ is the starting set of some $s \in Q$ then
        Compute $x[k] = s \in Q$ such that $St = S(s)$.
    else break;
    end if;
    $M := (\beta s)^{-1} \cdot M$;
end while;
return $z = \delta_n^{-p} x[1] \cdots x[k]$;
```

For the purpose of comparability with the success rates of the Lee-Park algorithm (without self-correction), we constrained the inputs to Artin positive braids. The table 3.4 shows the experimental results for the algorithms 3.2 and 3.5. On input (n, l), the program chooses at random 10000 x's from B_n^+ with $|x| = l_{\Omega_1}(x) = l$, computes $\rho_B(x)$ from x, computes z from $\rho_B(x)$ by each algorithm, and then checks whether or not z is equal to x by comparing their normal forms. Further, we compare algorithm 3.5 with algorithm 2.2 where we have set $t = 1$. Since, in this case, we deal with $\binom{n}{2}$-dimensional matrices, we performed just 1000 experiments per (n, l)-value.

TABLE 3.4 Success rate of recovering x from $\beta(x)$ (unit: %)

n	5			7			10		
$\|x\|$	30	40	50	40	55	70	60	80	100
Alg. 3.2	91.57	81.52	71.12	89.08	74.06	56.56	84.16	67.37	50.22
Alg. 3.5	95.49	90.16	83.87	92.67	81.72	68.76	88.49	72.86	55.75
Alg.2.2 $(t = 1)$	95.5	91.2	84.8	93.0	82.3	67.4	88.3	73.9	52.8

Observation: The success rates of our linear complexity inverting heuristic for the Burau representation are slightly, but significantly, better than the corresponding success rates of the Hughes or the Lee-Park algorithm (without self-correction) for all investigated parameter values. Further, the success rates of algorithm 3.5 and algorithm 2.2 with $t = 1$ are roughly equal. Since the Lawrence-Krammer module for $t = 1$ is the symmetric square of the (reduced) Burau module, this is far from being a surprising effect.
But the success rates of algorithm 3.3 are not within reach for our algorithm 3.5. This is due to a lack of self-correction in this algorithm. The development of a self-correcting version of algorithm 3.5 remains as a task for future research. Nevertheless, since algorithm 3.5 has linear time complexity (as Hughes' algorithm), it can be used as a cryptanalytic tool in representation attacks against braid-based cryptosystems.

Note that success rates of all inversion algorithms for the Burau representation are 100% for the 3-strand braid group. But they are lower than 100% in the case $n = 4$. This also holds for algorithm 2.2 setting $t = 1$. This confirms the conjecture that the Burau representation is not faithful for $n = 4$. But non-trivial Burau kernel elements in B_4 have not been found so far. According to an exhaustive search, using the topological characterization of Burau kernel elements reported in **[Bi99]**, such elements, if they really exist, must be quite long "monster elements".

Chapter 4

Representation attacks on the braid Diffie-Hellman key agreement

4.1 Braid Diffie-Hellman key agreement

Braid-based cryptography was introduced by Anshel, Anshel and Goldfeld in 1999 [**AAG99**] and by Ko, Lee, Cheon, Han, Kang and Park at the CRYPTO 2000 [**KL$^+$00**]. Several attacks have been proposed for the AAG key agreement protocol (KAP) for braid groups, and for the Ko, Lee et al. protocol so far. We will discuss them in detail in chapter 5. Further, an introducing, summarizing and outlooking survey on braid-based cryptography is given by P. Dehornoy [**De04b**].
Here we deal with the braid Diffie-Hellman KAP suggested at the ASIACRYPT 2001 [**CK$^+$01**], which is an revised version of the Ko-Lee protocol [**KL$^+$00**]. A straightforward generalization for general groups is described in section 5.2.1.
Let LB_m and UB_{n-m} $(m < n)$ be the commuting subgroups of B_n generated by $\sigma_1, \ldots, \sigma_{m-1}$ and $\sigma_{m+1}, \ldots, \sigma_{n-1}$ respectively. The elements of LB_m and UB_{n-m} are called lower and upper braids. Now, Alice and Bob have to perform the following protocol steps:

0. Alice or Bob select (and publish) a generic, sufficiently complicated braid $x \in B_n$.
1.A Alice generates randomly $(a_l, a_r) \in LB_m^2$, and sends $y_A = a_l x a_r$ in a rewritten (normal) form to Bob.
1.B Bob generates randomly $(b_l, b_r) \in UB_{n-m}^2$, and sends a rewritten form of $y_B = b_l x b_r$ to Alice.

2.A Alice receives y_B and computes $K := a_l y_B a_r$.

2.B Bob receives y_A and computes also the shared key $b_l y_A b_r = b_l(a_l x a_r)b_r = a_l(b_l x b_r)a_r = a_l y_B a_r = K$.

The security of this key agreement scheme and the corresponding public key cryptosytem[1] (PKC) depend on the following specific Diffie-Hellman type Decompositon Problem (DH-DP) for braid groups:

Input: $(x, y_A, y_B) \in B_n^3$ such that $y_A = a_l x a_r$ and $y_B = b_l x b_r$ for some $a_l, a_r \in LB_m$ and $b_l, b_r \in UB_{n-m}$.
Objective: Find $K := a_l y_B a_r = b_l y_A b_r = a_l b_l x a_r b_r$.

To recover the private key $(a_l, a_r) \in LB_m^2$ of Alice it is sufficient to solve the following specific Decompositon Problem (DP) for braid groups:

Input: $(x, y_A) \in B_n^2$ such that $y_A = a_l x a_r$ for some $a_l, a_r \in LB_m$.
Objective: Find $(a_l', a_r') \in LB_m^2$ such that $a_l' x a_r' = y_A$.

A solution for the DP induces a solution for the DH-DP. In the case $a_l = a_r^{-1}$ and $b_l = b_r^{-1}$ we obtain the original braid Diffie-Hellman key agreement scheme, which is based on a Diffie-Hellman version of the Generalized Conjugacy Search Problem (GCSP) [**KL**$^+$**00**] (see section 5.1.2). The fact that in general $a_l \neq a_r^{-1}$ (and $b_l \neq b_r^{-1}$) for the revised scheme [**CK**$^+$**01**] is indeed its advantage: x and y_A are in general not in the same conjugacy class. So attacks which (frequently) use conjugacy operations like cycling attacks [**HS03**] and Gebhardt's computation of Ultra Summit Sets [**Ge05**, **Ge06**] do not work.
We can restrict to the monoid versions DP$^+$ and DH-DP$^+$, in which each braid group is replaced by the corresponding monoid of positive braids, because we can multiply the equations $y_A = a_l x a_r$, $y_B = b_l x b_r$ by a sufficiently high power of the square of the Garside element Δ_n^2, which generates the center of B_n.

4.2 Representation attacks and previous work

Linear algebra or representation attacks on braid-based cryptosystems work as follows:

I. Choose a linear representation $\rho : B_n \longrightarrow GL(k, R)$ of the n-braid group for some ring R and $k \in \mathbb{N}$, and compute the images of the instance braids for this representation.

[1] Using an ideal hash function from the braid group into the message space $H : B_n \longrightarrow \{0,1\}^k$ a corresponding Public Key Encryption can be constructed ([**CK**$^+$**01**], chapter 6).

II. Solve the base problem in the matrix group $GL(k,R)$. Keep in mind that there will be infinitely many solutions in general, and that not all solutions are in $\mathrm{im}\rho \subset GL(k,R)$.

III. Find preimage braids for solutions in $\mathrm{im}\rho$.

4.2.1 Linear algebra attack on DH-DP via Lawrence-Krammer representation

Here we describe the deterministic polynomial time algorithm developed by J. H. Cheon and B. Jun [**CJ03a**, **CJ03b**].
Let V denote the free $\mathbb{Z}[t^{\pm1},q^{\pm1}]$-module of rank $\binom{n}{2}$ with basis $\{x_{ij} | 1 \le i < j \le n\}$ (see section 2.2). Via Lawrence-Krammer (LK) representation [**La90**] $\rho = \rho_n : B_n \longrightarrow GL(\binom{n}{2}, \mathbb{Z}[t^{\pm1},q^{\pm1}]) = Aut(V)$ braids acts on V. Recall that the action of an Artin generator σ_k $(k = 1,\dots,n-1)$ is given by

$$(\rho_n\sigma_k)x_{ij} = \begin{cases} tq^2x_{k,k+1}, & i=k, j=k+1 \\ (1-q)x_{ik} + qx_{i,k+1}, & i<k=j \\ x_{ik} + tq^{k-i+1}(q-1)x_{k,k+1}, & i<k, j=k+1 \\ tq(q-1)x_{k,k+1} + qx_{k+1,j}, & i=k, k+1<j \\ x_{kj} + (1-q)x_{k+1,j}, & i=k+1<j \\ x_{ij}, & j<k \quad \text{or} \quad k+1<i \\ x_{ij} + tq^{k-i}(q-1)^2x_{k,k+1}, & i<k, k+1<j. \end{cases}$$

$\rho_n b$ denotes the LK matrix of the braid $b \in B_n$ according to this x-basis. Further, we use the abbreviation $\rho'_n := \rho_n|_{q=1/2}$. Now, the Cheon-Jun attack on DH-DP$^+$ works roughly as follows. For technical details see [**CJ03b**].

I. Compute $X = \rho'_n x, Y^A = \rho'_n y_A, Y^B = \rho'_n y_B \in Mat(\binom{n}{2}, \mathbb{Q}[t])$ for x, y_A, $y_B \in B_n^+$.

II. Compute $\binom{n}{2} \times \binom{n}{2}$-matrices A'_l, A'_r over $\mathbb{Q}[t]$ satisfying the following equations $\forall k = m+1,\dots,n-1$:

$$XA'_r = A'_lY^A \qquad (1)$$

$$\left.\begin{array}{rcl} \rho'_n(\sigma_k)A'_l &=& A'_l\rho'_n(\sigma_k) \\ \rho'_n(\sigma_k)A'_r &=& A'_r\rho'_n(\sigma_k) \end{array}\right\} \qquad (2)$$

A'_l is invertible with overwhelming probability, so we can compute $(A'_l)^{-1}Y^BA'_r = (A'_l)^{-1}(B^lXB^r)A'_r \overset{(2)}{=} B^l((A'_l)^{-1}XA'_r)B^r \overset{(1)}{=} B^lY^AB^r = \rho'_n(K)$ with $B^l := \rho'_nb_l, B^r := \rho'_nb_r$.
Note that in general $(A'_l)^{-1} \neq A^l := \rho'_na_l$ and $A'_r \neq A^r := \rho'_na_r$, and $(A'_l)^{-1}$ and A'_r need not to lie in im ρ'_n.
We remark that we can change the system (1), (2) by vectorization into

a highly overdetermined linear system with $(2n-2m-1)\binom{n}{2}^2$ equations and $2\binom{n}{2}^2$ variables, which are polynomials in $\mathbb{Q}[t]$. By precise analysis of Krammer matrices, as suggested in the proof of theorem 3 in [**CJ03b**], we can reduce the number of variables and equations. Nevertheless, here we have to correct a simple mistake in theorem 3 of [**CJ03b**]:

Let $n=2m$. Using a reordering of the basis $\rho'_n\sigma_k$ $(k=m+1,\ldots,n-1)$ can be written as $\left(\begin{smallmatrix} M_k & 0 \\ 0 & \mathrm{Id}\end{smallmatrix}\right)$ where M_k is a square matrix of size $k(n-k)+n-2=\binom{n}{2}-\binom{k-1}{2}-\binom{n-k-1}{2}$. Therefore, each matrix equation (2), for $n/2<k<n$, yields only $[k(n-k)+n-2]^2$ non-trivial equations, while Cheon and Jun claim that there are only $k(n-k)$ non-trivial equations (for $n/2<k<n$). We cannot follow this argument. To establish such a result a much more precise analysis of LK matrices of Artin generators would be necessary, if possible. But such an analysis is missing in the proof of theorem 3 in [**CJ03b**].

Therefore, the numbers of variables and equations in the above mentioned, highly overdetermined linear system keep (in the case $m=O(n)$) $O(n^4)$ and $O(n^5)$, respectively. The complexity of the Cheon-Jun attack is dominated by Gaussian elimination for such linear systems.

III. In section 3.2 of [**CJ03b**] Cheon and Jun developed a polynomial time algorithm for inverting the LK-representation based on the ideas of Krammer [**Kr02**] (see algorithm 2.1 described in section 2.4). Applying this algorithm to $(A'_l)^{-1}Y^BA'_r=\rho'_n(K)$ we obtain the unique preimage braid K.

Practically we can also use LK matrices according to standard fork basis and algorithm 2.2 as inverting algorithm. But in this case we have no proof that the algorithm is deterministic.

So the Cheon-Jun attack provides a deterministic polynomial time solution to the DH-DP. Nevertheless the complexity is too large to break the cryptosystem with the proposed parameters in [**KL$^+$00**, **CK$^+$01**] efficiently. A complexity analysis of the Cheon-Jun attack is given in section 4.3.3.

4.2.2 Linear algebra attack on DP via Burau representation

In this section we describe a linear algebra attack using the Burau representation, introduced by E. Lee and J. Park in [**LP03**].

Let W_0 denote the free $\mathbb{Z}[q^{\pm1}]$-module of rank n with basis $\{w_i|1\leq i\leq n\}$.

The (unreduced)[2] Burau representation [**Bu36**] $\beta_n : B_n \longrightarrow GL(n, \mathbb{Z}[q^{\pm 1}]) = Aut(W_0)$ defined by

$$\beta_n \sigma_k = \mathrm{Id}_{k-1} \oplus \begin{pmatrix} 1-q & q \\ 1 & 0 \end{pmatrix} \oplus \mathrm{Id}_{n-k-1} \qquad \forall\, k = 1, \ldots, n-1$$

provides the following special attack on DP$^+$, but only in the symmetric case $2m = n$:

I. Compute $X = \beta_n x, Y = \beta_n y_A \in Mat(n, \mathbb{Z}[q])$ for $x, y_A \in B_n^+$.

II. Consider the DP-induced decomposition $W_0 = \mathrm{span} L \oplus \mathrm{span} U$ with $L := \{w_i | 1 \leq i \leq m\}, U := \{w_i | m+1 \leq i \leq n\}$. Then we obtain the following block matrix equations:

$$\begin{aligned} Y = \begin{pmatrix} Y_{LL} & Y_{LU} \\ Y_{UL} & Y_{UU} \end{pmatrix} &= \begin{pmatrix} A_l & 0 \\ 0 & \mathrm{Id}_{n-m} \end{pmatrix} \begin{pmatrix} X_{LL} & X_{LU} \\ X_{UL} & X_{UU} \end{pmatrix} \begin{pmatrix} A_r & 0 \\ 0 & \mathrm{Id}_{n-m} \end{pmatrix} \\ &= \begin{pmatrix} A_l X_{LL} A_r & A_l X_{LU} \\ X_{UL} A_r & X_{UU} \end{pmatrix} \end{aligned}$$

Note that $A_l = \beta_m a_l, A_r = \beta_m a_r$. In the case $2m = n$ the offdiagonal blockmatrices X_{LU}, X_{UL} are quadratic. The probability that X_{LU} or X_{UL} have full rank for randomly chosen $x \in B_n^+$ increases for $n = \mathrm{const}$ and increasing word length $|x|$, and for $|x| = \mathrm{const}$ and decreasing braid index n ($n \geq 5$) [**LP03**]. If at least one of these two offdiagonal matrices is regular, so we obtain $A_l = Y_{LU} X_{LU}^{-1}$ or $A_r = X_{UL}^{-1} Y_{UL}$.

In numerous experiments the probabilities that X_{LU} or X_{UL} are regular were found to be 90% or so for $cl(x) = l_\Omega(x) = 5$ and $n = 50, 70, 90$ (see section 4.3 in [**LP03**]).

In [**Ko03**] Ko suggests the following countermeasure: Choose a x which contains just a few generators σ_m.

III. The Burau representation is proved to be not faithful for $n \geq 5$ [**Bi99**]. The only known algorithms for computing preimage braids for the Burau representation are the heuristic Hughes algorithm [**Hu02**] and its variations by Lee and Park [**LP03**] (see chapter 3). Applying it to A_l or A_r, we might obtain a_l or a_r, and that is sufficient to solve DP.

Since the self-correcting algorithm 3.3, which provides the best success rates so far, took too long time to be used on a PC for large parameters, Lee and Park used algorithm 3.2 to compute preimage braids for the Burau representation. Let $a = a_l$ or a_r. For the parameter values $(n, cl(a)) = (50, 3), (70, 3)$ and $(90, 3)$ a is recovered from $\beta_m(a)$ with a success rate of 100%. Further, Lee and Park can recover a from

[2] It is also possible to use the reduced Burau representation $B_n \longrightarrow GL(n-1, \mathbb{Z}[q^{\pm 1}])$.

$\beta_m(a)$ for $(n, cl(a)) = (50, 5)$, $(70, 5)$, $(90, 5)$ and $(50, 10)$ with significant probability [**LP03**]. These results can be even improved by using our inverting algorithm 3.5 instead of Lee, Park's algorithm 3.2. Nevertheless, the success rates of these heuristics decrease for $m =$ const with increasing word length $|a|$ (or canonical length $cl(a)$), and they are very low for the parameter values suggested in [**CK$^+$01**].

4.3 Probabilistic linear algebra attack using Lawrence-Krammer representation

Now we use ideas from Lee and Park [**LP03**] to develop an attack on DP$^+$ via LK representation. For generic and sufficiently long instance braids we recover the ρ'_m-image of Alice's private key by using just[3] one matrix inversion. We have already published this work in [**Ka06**].

4.3.1 Symmetric case $2m = n$

Consider the DP-induced decomposition $V = \operatorname{span} L \oplus \operatorname{span} M \oplus \operatorname{span} U$ with $L := \{x_{ij} | 1 \le i < j \le m\}, M := \{x_{ij} | 1 \le i \le m < m+1 \le j \le n\}$ and $U := \{x_{ij} | m+1 \le i < j \le n\}$ ($|L| = \binom{m}{2}, |M| = m(n-m), |U| = \binom{n-m}{2}$). The basis is reordered according to the DP-induced decomposition of V by the transformation $\phi : \{x_{ij} | 1 \le i < j \le n\} \longrightarrow \{x_k | 1 \le k \le \binom{n}{2}\}$ defined by $x_{ij} \mapsto x_k$ with

$$k := \begin{cases} \binom{j-1}{2}, & x_{ij} \in L \\ \binom{m}{2} + (j-m-1)m + i, & x_{ij} \in M \\ \binom{m}{2} + m(n-m) + \binom{j-m-1}{2} + i - m, & x_{ij} \in U \end{cases}$$

So we get the following block matrix structures for embedded braids:

$$\rho_n a = \begin{pmatrix} A_{LL} & A_{LM} \\ 0 & A_{MM} \end{pmatrix} \oplus \mathrm{Id}_{\binom{n-m}{2}} \quad \forall a \in LB_m \quad \text{and}$$

$$\rho_n b = \mathrm{Id}_{\binom{m}{2}} \oplus \begin{pmatrix} B_{MM} & 0 \\ B_{UM} & B_{UU} \end{pmatrix} \quad \forall b \in UB_{n-m}\,.$$

Note that $A_{LL} = \rho_m a = \rho_m a(t, q)$, $A_{LM} = A_{LM}(t, q)$, rank $A_{LM} \le m$, and $A_{MM} = A_{MM}(q) = (\tilde{\beta}_m a)^{\oplus(n-m)} \in Mat((n-m)m, \mathbb{Z}[q^{\pm 1}])$, where $\tilde{\beta}_m : B_m \to GL(m, \mathbb{Z}[q^{\pm 1}])$ is a Burau-type representation.

[3] Nevertheless, this matrix is an $\binom{m}{2}$-dimensional matrix over $\mathbb{Q}[t]$.

TABLE 4.1: $p := \text{Prob}(\text{rank}\, X_{UL}|_{t=3} = \binom{m}{2})$

$n = 2m$									
6	$\lvert x\rvert$	15	20	25	30	35	40	45	50
	p in %	6	30	41	62	77	90	92	95
8	$\lvert x\rvert$	30	40	50	60	70	80	90	100
	p in %	0	7	30	48	69	87	89	99
10	$\lvert x\rvert$	70	90	110	130	150	170		
	p in %	5	21	60	80	92	100		
12	$\lvert x\rvert$	100	140	180	220	260			
	p in %	1	20	65	88	99			

100 random experiments were executed for each entry. A randomly chosen $x \in B_n^+$ is rejected, if it does not contain all Artin generators.

The commutativity equation $ab = ba \quad \forall a \in LB_m \forall b \in UB_{n-m}$ yields the following block matrix equation:

$$\rho_n ab = \begin{pmatrix} A_{LL} & A_{LM}B_{MM} & 0 \\ 0 & A_{MM}B_{MM} & 0 \\ 0 & B_{UM} & B_{UU} \end{pmatrix} = \begin{pmatrix} A_{LL} & A_{LM} & 0 \\ 0 & B_{MM}A_{MM} & 0 \\ 0 & B_{UM}A_{MM} & B_{UU} \end{pmatrix}.$$

Our representation attack contains the following steps:

I. Compute the images of the instance braids:

$$\rho'_n x = \begin{pmatrix} X_{LL} & X_{LM} & X_{LU} \\ X_{ML} & X_{MM} & X_{MU} \\ X_{UL} & X_{UM} & X_{UU} \end{pmatrix}, \rho'_n y_A = \begin{pmatrix} Y_{LL} & Y_{LM} & Y_{LU} \\ Y_{ML} & Y_{MM} & Y_{MU} \\ Y_{UL} & Y_{UM} & Y_{UU} \end{pmatrix}.$$

II. The UL-block matrix from $\rho'_n a_l x a_r =$

$$\left(\begin{array}{c|c|c} A^l_{LL}X_{LL}A^r_{LL}+ & (A^l_{LL}X_{LL}+A^l_{LM}X_{ML})A^r_{LM}+ & A^l_{LL}X_{LU}+ \\ A^l_{LM}X_{ML}A^r_{LL} & (A^l_{LL}X_{LM}+A^l_{LM}X_{MM})A^r_{MM} & A^l_{LM}X_{MU} \\ \hline A^l_{MM}X_{ML}A^r_{LL} & A^l_{MM}(X_{ML}A^r_{LM}+X_{MM}A^r_{MM}) & A^l_{MM}X_{MU} \\ \hline X_{UL}A^r_{LL} & X_{UL}A^r_{LM}+X_{UM}A^r_{MM} & X_{UU} \end{array}\right)$$

yields the equation $Y_{UL} = X_{UL}A^r_{LL}$.
X_{UL} is quadratic for $2m = n$ and non-singular with increasing probability for increasing $|x|$ ($n =$ const) and decreasing n ($|x| =$ const) (see table 4.1).
If X_{UL} is regular, we can compute $\rho'_m a_r = A^r_{LL} = X_{UL}^{-1}Y_{UL}$.
If it is not, choose a generic, sufficiently long $u \in UB^+_{n-m}$ with $\rho'_n u =$

$\mathrm{Id}_{\binom{m}{2}} \oplus \begin{pmatrix} U_{MM} & 0 \\ U_{UM} & U_{UU} \end{pmatrix}$, and compute

$$\begin{aligned}(\rho'_n u a_l x a_r)_{UL} &= (UY)_{UL} = U_{UM}Y_{ML} + U_{UU}Y_{UL} = U_{UM}A^l_{MM}X_{ML}A^r_{LL} \\ &\qquad + U_{UU}X_{UL}A^r_{LL} \overset{(3)}{=} (U_{UM}X_{ML} + U_{UU}X_{UL})A^r_{LL}.\end{aligned}$$

Then $U_{UM}X_{ML} + U_{UU}X_{UL} = (\rho'_n ux)_{UL}$ has with high probability full rank for sufficiently long u, and we obtain

$$A^r_{LL} = (U_{UM}X_{ML} + U_{UU}X_{UL})^{-1}(U_{UM}Y_{ML} + U_{UU}Y_{UL}).$$

Note that this regularization procedure does not work, if X_{ML} and X_{UL} have a common zero column, or if X_{UL} is the null matrix and X_{ML} does not have full rank. But for generic, sufficiently long and complicated x, which of course contains all Artin generators $\sigma_1, \ldots, \sigma_{n-1}$, this will not occur.

III. By Cheon-Jun algorithm we lift back $A^r_{LL} = \rho'_m a_r$ to $a_r \in B^+_m$.

4.3.2 Asymmetric cases

(a) The case $m < n - m$

Here we have to replace m by $m' := n/2$ (n even) or $m' := (n+1)/2$ (n odd) in the definitions of L, M, U. If n is even the problem is reduced to the symmetric case $n = 2m'$.
But if n is odd we have to embed the problem into $B_{2m'}$ and compute images of the instance braids for $\rho'_{2m'}$. Choose the decomposition $\mathrm{span}\{x_{ij} | 1 \le i < j \le 2m'\} = \mathrm{span}L \oplus \mathrm{span}\bar{M} \oplus \mathrm{span}\bar{U}$ with $\bar{M} := \{x_{ij} | 1 \le i \le m', m'+1 \le j \le 2m'\}$ and $\bar{U} := \{x_{ij} | m'+1 \le i < j \le 2m'\}$. Then $X_{\bar{U}L}$ is quadratic, but singular - it contains (at least) $m' - 1 = (n-1)/2$ zero rows, and $X_{\bar{M}L}$ has (at least) $m' = (n+1)/2$ zero rows. Nevertheless we can apply the above regularization procedure again:
Choose a generic, sufficiently long $u \in \bar{U}B^+_{2m'-m'} := \langle \sigma_{m'+1}, \ldots, \sigma_{2m'-1}\rangle^+ \subset B^+_{2m'}$ and compute

$$\begin{aligned}(\rho'_{2m'} u y_A)_{\bar{U}L} &= U_{\bar{U}\bar{M}}Y_{\bar{M}L} + U_{\bar{U}\bar{U}}Y_{\bar{U}L} = U_{\bar{U}M}Y_{ML} + U_{\bar{U}U}Y_{UL} = \\ (\rho'_{2m'} u a_l x a_r)_{\bar{U}L} &= (\rho'_{2m'} u x a_r)_{\bar{U}L} = (U_{\bar{U}\bar{M}}X_{\bar{M}L} + U_{\bar{U}\bar{U}}X_{\bar{U}L})A^r_{LL} \\ &= (U_{\bar{U}M}X_{ML} + U_{\bar{U}U}X_{UL})A^r_{LL}.\end{aligned}$$

$(\rho'_{2m'} ux)_{\bar{U}L} = U_{\bar{U}M}X_{ML} + U_{\bar{U}U}X_{UL}$ is quadratic, and regular for generic, sufficiently long $u \in \bar{U}B'^+_m, x \in LB^+_n$, and we obtain

$$A^r_{LL} = (U_{\bar{U}M}X_{ML} + U_{\bar{U}U}X_{UL})^{-1}(U_{\bar{U}M}Y_{ML} + U_{\bar{U}U}Y_{UL}) = \rho'_{m'} a_r.$$

(b) The case $m > n - m$

By half twist transformation $\tau_n : B_n \longrightarrow B_n$ def. by $\sigma_i \mapsto \sigma_{n-i}$ we reduce case (b) to case (a).
Note that we perform now an attack on Bob's private key, while in case (a) we only can compute the private key of Alice.

(c) Simple Generalizations

We can introduce some simple variations and generalizations of the DH-DP: One way is to choose different partitions of the (l)eft and (r)ight "areas," i.e. choose $a_l \in LB_{m_l}, b_l \in UB_{n-m_l}, a_r \in LB_{m_r}, b_r \in UB_{n-m_r}$ with $m_l \neq m_r$ $(m_l, m_r < n)$. By half twist transformation, reverse anti-automorphism of B_n and proper embeddings of the private keys we can transform the problem to the following standard form of l,r-asymmetric DP:

INSTANCE: $(x', y') \in B_n^2$ such that $y' = p_l x p_r$ for some $p_l \in LB_{m'_l}, p_r \in LB_{m'_r}$ with $m'_r = n - m'_l < n/2$.
OBJECTIVE: Find $p'_l \in LB_{m'_l}, p'_r \in LB_{m'_r}$ such that $p'_l x' p'_r = y'$.

Defining $L := \{x_{ij} | 1 \leq i < j \leq m'_r\}$ and $U := \{x_{ij} | n - m'_r + 1 \leq i < j \leq n\}$ we get $(\rho'_n y')_{UL} = (\rho'_n p_l x' p_r)_{UL} = X'_{UL}\rho'_{m'_r}(p_r)$. So recovering p_r depends on the regularity of the quadratic block matrix $X'_{UL} := (\rho'_n x')_{UL}$.
Another way is to choose $a_r \in UB_{n-m}, b_r \in LB_m$ (and keep $a_l \in LB_m, b_l \in UB_{n-m}$) or vice versa. But in this case we can attack the DP, if one of the quadratic matrices X_{UU} or X_{LL} is invertible.
Further generalizations e.g., by introducing refined partitions of each "area," can be treated with similar methods.

4.3.3 Complexity analysis

For simplicity we assume that $x, y_A \in B_{2m}^+$, $a_l, a_r \in LB_m^+$, and x, a_l, a_r have the same (Artin) canonical length l. Therefore the entries in $A^r_{LL} = \rho'_m a_r$ are polynomials in $\mathbb{Q}[t]$ with degree bounded above l. According to Corollary 1 in **[CJ03b]** the absolute values of the numerators and denominators of the coefficients of these polynomials are bounded by $2^{|a_r|}$ and $2^{2(m-1)l}$ respectively. Let p be a prime with $p > 2^{|a_r|+2(m-1)l}$ and $f(t)$ an irreducible polynomial of degree l over $\mathbb{Z}_p$. Then we have

$$\rho'_m a_r = \frac{1}{2^{2(m-1)l}}[2^{2(m-1)l}\rho'_m a_r \mod(p, f(t))].$$

So we can work in the residue class field $F = \mathbb{Z}_p[t]/(f) \cong \mathbb{F}_{p^l}$ rather than in $\mathbb{Q}[t]$. This allows us to estimate the costs of the ring operations. Using

Schönhage-Strassen method one multiplication in $\mathbb{Z}_p$ takes $O(\log p \log\log p \log\log\log p) = O^{\sim}(\log p) = O^{\sim}(|a_r|) = O^{\sim}(m^2 l)$ bit operations[4], and a multiplication in $\mathbb{F}_{p^l}$ takes $O(l^2)$ multiplications in $\mathbb{Z}_p$[5]. Therefore an operation in F takes $O^{\sim}(l^2 \log p) = O^{\sim}(m^2 l^3)$ bit operations.

Step II: Compute $\rho'_m a_r = X_{UL}^{-1} Y_{UL}$.

The matrix inversion has the same asymptotic complexity of $O(m^{2\tau})$ operations in F as matrix multiplication. The feasible matrix multiplication exponent τ is 3 for classical algorithms, $\log_2 7$ using Strassen's method, and the current world record is $\tau < 2.376$ (**[GG99]**, section 12.1). Therefore the asymptotic complexity of step II is about $O^{\sim}(m^{2\tau+2} l^3)$.

Step III: Invert the Lawrence-Krammer representation.

In **[CJ03b]** the authors errouneously assume that the complexity of their Algorithm 1 for inverting the Lawrence-Krammer representation is dominated by the computation of a power of $\rho_n \Delta_n$. This is not the case, because we can compute even powers by formula $\rho_n \Delta_n^{2k} = t^{2k} q^{2nk} \mathrm{Id}_{\binom{n}{2}}$ and $\rho_n \Delta_n$ is sparse - it has the support of a permutation matrix.

Therefore the complexity of the Cheon-Jun algorithm (Algorithm 1 in **[CJ03b]**) is dominated by step 3.4 (for $k = 1$ to l). So Inverting $A^r_{LL} = \rho'_m a_r$ has the same complexity as computing $\rho'_m a_r$[6].

In step 3.4 we have to perform $O((m^2)^\tau)$ operations in F. That are $O(m^{2\tau} l)$ operations in $\mathbb{Z}_p$, because the (Artin) canonical length of a permutation braid is 1. Therefore step 3.4 takes $O^{\sim}(m^{2\tau} l \log p) = O^{\sim}(m^{2\tau+2} l^2)$ and the whole Algorithm 1 $O^{\sim}(m^{2\tau+2} l^3)$ bit operations.

Note that the computation of the Krammer matrices of l permutation braids takes $O^{\sim}(m^6 l)$ bit operations:

The Krammer matrix of an Artin generator contains at most 2 nonzero entries per column. So multiplication with $\rho'_m \sigma_j$ $(j = 1, \ldots, m-1)$ takes $O((m^2)^2)$ field operations in F, and also in $\mathbb{Z}_p$, because the (Artin) canonical length of a permutation braid is 1. Because the word length of a permutation braid b_σ is $O(m^2)$, Schönhage-Strassen multiplication takes $O^{\sim}(|b_\sigma|) = O^{\sim}(m^2)$ bit operations.

Summary: Our proposed attack requires $O^{\sim}(m^{2\tau+2} l^3)$ bit operations using

[4] For a precise definition of the $O^{\sim}$-notation see definition 25.8 in **[GG99]**.

[5] Using asymptotically fast algorithms this can be reduced to $O^{\sim}(l)$ multiplications in $\mathbb{Z}_p$.

[6] Because the (Artin) canonical length of y_A is bounded by $3l$, step I (compute $\rho'_n x, \rho'_n y_A$) has the same complexity as step III.

Schönhage-Strassen multiplication in $\mathbb{Z}_p$ and $O(m^{2\tau+4}l^4)$ bit operations using classical multiplication.

Comparison with Cheon-Jun attack: The complexity of Cheon-Jun atack **[CJ03b]** is dominated by Gaussian elimination. The Gaussian elimination of the overdetermined system with $O(m^5)$ equations and $O(m^4)$ variables needs $O(m^{5\tau})$ operations in F, and therefore $O^{\sim}(m^{5\tau+2}l^3)$ bit operations using Schönhage-Strassen multiplication and $O(m^{5\tau}l^2(m^2l)^2) = O(m^{5\tau+4}l^4)$ bit operations using classical multiplication.
Therefore, our attack is 3τ orders in m (or n) more efficient than the Cheon-Jun attack.

Chapter 5

Braid group cryptography

Most of the currently used methods in public-key cryptography are based on problems in number theory. These methods have proved to be worthwhile over several years. Nevertheless, after the advent of quantum computers, systems like RSA [**RSA78**] and its variants, e.g. [**Ra79**] , ElGamal [**El85**] and ECC [**Mi85**, **Ko87**] will be broken easily [**Sh97**, **PZ03**].
There have been several efforts to develop public-key cryptosystems which are not based on number-theoretic problems. One approach is the use of hard problems in combinatorial group theory like the word problem [**De11**, **Th14**, **GZ91**], the conjugacy problem [**De11**], etc. The groups in question are usually non-commutative. Therefore, it was suggested to name this relatively new branch of cryptography as ”non-commutative cryptography” [**GG$^+$06**].
The first PKC that uses non-commutative groups was proposed by Wagner and Magyarik [**WM85**]. The platform groups are finitely presented groups with an unsolvable word problem. Such groups exist according to the Novikov-Boone theorem [**Bo54**, **No55**]. Some examples for such groups are given in [**La79**, **Co89**]. Furthermore there exist an efficient algorithm, which constructs from a finitely presented Thue system T with unsolvable word problem a finitely presented group $G(T)$ with unsolvable word problem. Note that the existence of finitely presented Thue systems with unsolvable word problem is guaranteed by the Post-Markov theorem [**Po47**, **Ma47**, **Ma86**]. Nevertheless, Birget, Magliveras and Sramka argued in [**BMS06**] that the Wagner-Magyarik scheme is based on the word choice problem rather than the word problem as proposed by the authors.
A cryptosystem using Lyndon words was proposed by Siromoney and Mathew [**SM90**].
According to a theorem of C. Miller III [**Mi71**] there exist finitely presented, residually finite groups with algorithmically unsolvable conjugacy problem. Since these groups are residually finite, they have a solvable word problem.

An earlier example for a finitely presented group with solvable word problem, but unsolvable conjugacy problem, was given in [**Fr60**]. A PKC based on Miller's theorem was introduced in [**AA93**]. Note that an analogue critique as in [**BMS06**] applies also to the scheme proposed in [**AA93**]. In particular, the scheme is not based on the conjugacy problem, but on the conjugacy choice problem, which we define analogously to the word choice problem described in [**BMS06**].
In 1999 I. Anshel, M. Anshel and Goldfeld described an key agreement protocol [**AAG99**] using noncomutative groups with feasible word problem, but algorithmically hard conjugacy problem. This was the first cryptosystem, where braid groups were explicitly suggested as platform groups. Therefore the paper [**AAG99**] marks the birthdate of braid group cryptography.
The introduction of the first braid-based cryptographic schemes [**AAG99**, **KL+00**, **CK+01**] caused some excitement in the crypto community and led to an amuont of cryptanalytic research. Further, braid group cryptography inspired the search for other feasible, non-commutative platform groups [**PH+01**, **PK+01**, **MST02**, **EK04**, **SU05**], or other non-commutative structures usable for cryptographic purposes (see, e.g., [**GP04**, **AK06**, **CDW07**]).

5.1 AAG and KLCHKP key agreement

5.1.1 Protocols

For the general AAG key agreement protocol for monoids [**AAG99**] we need two feasible monoids $(M, \cdot_M), (N, \cdot_N)$, and functions

$$\beta : M \times M \longrightarrow N, \quad \gamma_i : M \times N \longrightarrow N \quad (i = 1, 2)$$

which satisfy the following conditions:

(1) $\beta(x, \cdot) : M \to N$ is for all $x \in M$ a monoid homomorphism, i.e.

$$\forall x, y_1, y_2 \in M : \quad \beta(x, y_1 \cdot_M y_2) = \beta(x, y_1) \cdot_N \beta(x, y_2).$$

(2) It is, in general, not feasible to determine a secret $x \in M$ from the knowledge of

$$y_1, y_2, \ldots, y_k \in M \quad \text{and} \quad \beta(x, y_1), \beta(x, y_2), \ldots, \beta(x, y_k) \in N.$$

(3) For all $x, y \in M : \quad \gamma_1(x, \beta(y, x)) = \gamma_2(y, \beta(x, y)).$

Now Alice and Bob have to perform the following protocol steps:

0. Alice and Bob select two public submonoids

$$S_A = \langle s_1, \ldots, s_m \rangle, S_B = \langle t_1, \ldots, t_n \rangle \subset M.$$

1.A. Alice generates her secret key $a \in S_A$.

1.B. Bob chooses his secret key $b \in S_B$.

2.A. Alice computes the elements $\beta(a, t_1), \ldots, \beta(a, t_n)$ and publicly announces this list. This list is her public key.

2.B. Analogously Bob computes the elements $\beta(b, s_1), \ldots, \beta(b, s_m)$ and publishes this list. This list is his public key.

3.A. Alice, knowing $a = r_1 \cdots r_k$ with $r_i \in \{s_1, \ldots, s_m\}$, computes from Bob's public key

$$\beta(b, a) = \beta(b, r_1 \cdots r_k) \overset{(1)}{=} \beta(b, r_1) \cdots \beta(b, r_k).$$

3.B. And Bob, knowing $b = u_1 \cdots u_{k'}$ with $u_j \in \{t_1, \ldots, t_n\}$, computes from Alice's public key

$$\beta(a, b) = \beta(a, u_1 \cdots u_{k'}) \overset{(1)}{=} \beta(a, r_1) \cdots \beta(a, u_{k'}).$$

4.A. Alice computes $K := \gamma_1(a, \beta(b, a))$.

4.B. Bob also computes the shared key $\gamma_2(b, \beta(a, b)) \overset{(3)}{=} K$.

Note that, in order to establish a shared key K, it is sufficient to replace condition (3) by the weaker condition

(3') For all $a \in S_A, b \in S_B : \quad \gamma_1(a, \beta(b, a)) = \gamma_2(b, \beta(a, b))$.

In the following, monoids which are used in the AAG KAP, have to fulfill the conditions (1),(2) and (3').
The AAG key agreement scheme is formulated in a too general manner to be applied. For practical purposes we have to specify the monoids M, N and the functions $\beta, \gamma_1, \gamma_2$.
The AAG commutator KAP for groups [**AAG99**] is determined by the following specifications:
Let $M = N = G$ be a group, and S_A and S_B are assumed to be subgroups of G[1]. The functions $\beta, \gamma_1, \gamma_2 : G^2 \to G$ are defined by

$$\beta(x, y) = x^{-1}yx, \quad \gamma_1(x, y) = x^{-1}y, \quad \gamma_2(x, y) = y^{-1}x.$$

[1] Now r_i and u_j are elements from $\{s_1^{\pm 1}, \ldots, s_m^{\pm 1}\}$ and $\{t_1^{\pm 1}, \ldots, t_n^{\pm 1}\}$, respectively.

Note that the shared key is the commutator

$$K = \gamma_1(a, \beta(b,a)) = \gamma_1(a, b^{-1}ab) = a^{-1}(b^{-1}ab) = [a,b].$$

In combinatorial group theory multiplication is defined by simple concatenation of words. Therefore Alice and Bob have to publish the elements $\beta(a, t_i) = a^{-1}t_ia$ and $\beta(b, s_j) = b^{-1}s_jb$ in a disguised form. Therefore the question, whether one can efficiently disguise elements by using defining relations [**SZ06**], is very important for any platform group. One way is to use efficiently computable normal forms. Such normal forms exist, e.g., in braid group. Furthermore, the conjugator search, i.e. determining x from $\beta(x,y) = x^{-1}yx$, was assumed to be hard in braid groups. Therefore Anshel, Anshel and Goldfeld suggested braid groups as platform groups for the AAG commutator KAP [**AAG99**].
In 2000 Ko, Lee, Cheo, Han, Kang and Park introduced a new key agreement scheme based on braid groups [**KL$^+$00**]. Here we describe a generalized version of this KAP [**CK$^+$01**] for a general platform group G. Since this KAP is a non-abelian generalization of the classical Diffie-Hellman (DH) key agreement in the abelian group $\mathbb{F}_p^\times$ [**DH76**], we call it the group Diffie-Hellman key agreement protocol.

0. Alice and Bob select two public, commuting subgroups $S_A, S_B \subset G$, i.e. $[S_A, S_B] = 1$. Furthermore they publish a "generic" element $x \in G$.

1.A. Alice generates her secret key (a_l, a_r) with $a_l, a_r \in S_A$.

1.B. Bob selects his private key (b_l, b_r) with $b_l, b_r \in S_B$.

2.A. Alice computes $y_A = a_lxa_r$ and sends it to Bob.

2.B. Bob computes $y_B = b_lxb_r$ and submits it to Alice.

3.A. Alice receives y_B and computes $K := a_ly_Ba_r$.

3.B. Bob receives y_A and computes the shared key

$$b_ly_Ab_r = b_l(a_lxa_r)b_r = a_l(b_lxb_r)a_r = a_ly_Ba_r = K.$$

For $a_l = a_r^{-1}$ and $b_l = b_r^{-1}$ we obtain the original Ko-Lee et al. protocol [**KL$^+$00**].

Proposition 5.1 *The Ko-Lee protocol is a special case of Anshel Anshel Goldfeld KAP for monoids* [**AAG03**].

Proof. - Set $(M, \cdot_M) = (G, \cdot)$ and $N = \{g^{-1}xg \mid g \in G\}$. Furthermore define

$$1 \cdot_N u = u \cdot_N 1 = u \quad (\forall x \in N) \quad \text{and} \quad u \cdot_N v = u \quad (\forall u, v \in N, u \neq 1, v \neq 1).$$

This turns N into a monoid.
The functions $\beta : G^2 \to N$ and $\gamma_{1,2} : G \times N \to G$ are defined by

$$\beta(u, v) = u^{-1}xu, \quad \gamma_1(u, v) = \gamma_2(u, v) = u^{-1}vu.$$

Then condition (1) is fulfilled obviously, because $\beta(u, v)$ is independent of the second argument. Condition (2) is satisfied, because conjugacy search is assumed to be hard in the platform group G of the Ko-Lee protocol. And (3') holds, because we have for all $a \in S_A$, $b \in S_B$ ($[S_A, S_B] = 1$):

$$\gamma_1(a, \beta(b, a)) = \gamma_1(a, b^{-1}xb) = a^{-1}b^{-1}xba = b^{-1}(a^{-1}xa)b = \gamma_2(b, \beta(a, b)). \ \Box$$

If we want to verify the stronger but not necessary condition (3), then we have to define **[AAG03]**

$$\gamma_1(u, v) \;=\; \begin{cases} x & u \notin C(x) \cdot S_A, \\ x & u \in C(x) \cdot S_A \quad \text{and} \quad v \notin N_B, \\ u^{-1}vu & u \in C(x) \cdot S_A \quad \text{and} \quad v \in N_B. \end{cases}$$

$$\gamma_2(u, v) \;=\; \begin{cases} x & u \notin C(x) \cdot S_B, \\ x & u \in C(x) \cdot S_B \quad \text{and} \quad v \notin N_A, \\ u^{-1}vu & u \in C(x) \cdot S_B \quad \text{and} \quad v \in N_A. \end{cases}$$

Here $C(x)$ denotes the centralizer of x and $N_A := \{a^{-1}xa \mid a \in S_A\}$, $N_B := \{b^{-1}xb \mid b \in S_B\}$. Note that $u \in C(x) \cdot S_A \Leftrightarrow u^{-1}xu \in N_A$ and $u \in C(x) \cdot S_B \Leftrightarrow u^{-1}xu \in N_B$.

Proposition 5.2 *The group Diffie-Hellman key agreement protocol is a special case of the Anshel Anshel Goldfeld KAP for monoids.*

Proof. - Here we set $M = G^2$ and $N = \{g_1xg_2 \mid (g_1, g_2) \in G^2\}$. The composition in G^2 is defined componentwise, and $\cdot_N$ is defined as in the proof of Prop. 5.1. Now, if we define the functions $\beta : G^2 \times G^2 \to N$ and $\gamma_{1,2} : G^2 \times N \to N$ by

$$\beta((u_1, u_2), (v_1, v_2)) = u_1xu_2, \quad \gamma_1((u_1, u_2), v) = \gamma_2((u_1, u_2), v) = u_1vu_2,$$

then condition (1) is satisfied obviously. Further, condition (2) holds, because it is assumed to be hard for the group G to determine $a = (a_1, a_2) \in G^2$

from $\beta((a_1,a_2),b) = a_1xa_2$. And (3') is satisfied, because we have for all $a=(a_1,a_2)\in S_A$, $b=(b_1,b_2)\in S_B$ ($[S_A,S_B]=1$):

$$\gamma_1(a,\beta(b,a)) = \gamma_1(a,b_1xb_2) = a_1b_1xb_2a_2 = b_1(a_1x_2)b_2 = \gamma_2(b,\beta(a,b)). \quad \square$$

So we have proved that the group DH KAP is a special case of the AAG KAP for monoids. Nevertheless, not every special case is obvious. Indeed, the group DH KAP does not use the homomophy property (1) anyway. We close with a construction of a explicit public-key cryptosystem (PKC) for enciphering/deciphering messages from the AAG KAP. This is a straightforward generalization of the PKC in [**KL$^+$00**]. We assume that the monoids M,N satisfy the conditions (1)-(3). Let $\{0,1\}^k$ be the message space and $H:G\to\{0,1\}^k$ an ideal hash function.

1. **Key generation by Alice:**
   (a) Choose two public submonoids
   $$S_A = \langle s_1,\dots,s_m\rangle, S_B = \langle t_1,\dots,t_n\rangle \subset M.$$
   (b) Choose the private key $a\in S_A$.
   (c) Compute the public key $(y_a,\dots,y_n)\in N^n$ with $y_i=\beta(a,t_i)$.
2. **Encryption by Bob:**
   (a) Choose a $b\in S_B$ at random.
   (b) Compute $c_i=\beta(b,s_i)$ for all $i=1,\dots,m$.
   (c) Use the presentation $b=t_{i_1}\cdots t_{i_{|b|}}$ for the computation of
   $$\beta(a,b)=\beta(a,t_{i_1})\cdots\beta(a,t_{i_{|b|}}) = y_{i_1}\cdots y_{i_{|b|}}.$$
   (d) Encipher the message $m\in\{0,1\}^k$ by $d=m\oplus H(\gamma_2(b,\beta(a,b))$. The cipher text is $(c_1,\dots,c_m,d)$.
3. **Decryption by Alice:**
   (a) Use the presentation $a=s_{j_1}\cdots s_{j_{|a|}}$ for the computation of
   $$\beta(b,a)=\beta(b,s_{j_1})\cdots\beta(b,s_{j_{|a|}}) = c_{j_1}\cdots c_{j_{|a|}}.$$
   (b) Compute the original message by
   $$d\oplus H(\gamma_1(a,\beta(b,a))) = m\oplus H(\gamma_2(b,\beta(a,b)))\oplus H(\gamma_1(a,\beta(b,a))) \overset{(3)}{=} m.$$

5.1.2 Base problems

The following search problems are related with the group based protocols from the previous section:

CSP (Conjugacy Search Problem):
INPUT: $(s, s^x) \in G^2$.
OBJECTIVE: Find $x' \in G$ such that $s^{x'} = s^x$.

l-**SCSP** (l-Simultaneous Conjugacy Search Problem):
INPUT: $\{(s_i, s_i^x) \in G^2 | i = 1, \dots, l\}$.
OBJECTIVE: Find $x' \in G$ such that $s_i^{x'} = s_i^x \quad \forall i = 1, \dots, l$.

GCSP (Generalized Conjugacy Search Problem):
INPUT: $(s, s^x) \in G^2$ with $x \in T \subset G$.
OBJECTIVE: Find $x' \in T$ such that $s^{x'} = s^x$.

l-**SGCSP** (l-Simultaneous Generalized Conjugacy Search Problem):
INPUT: $\{(s_i, s_i^x) \in G^2 | i = 1, \dots, m\}$ with $x \in T \subset G$.
OBJECTIVE: Find $x' \in T$ such that $s_i^{x'} = s_i^x \quad \forall i = 1, \dots, l$.

AAGP (Anshel-Anshel-Goldfeld Problem):
INPUT: $\{(a_i, a_i^y) \in G^2 | i = 1, \dots, k\} \cup \{(b_j, b_j^x) \in G^2 | j = 1, \dots, m\}$ with $x \in A = \langle a_1, \dots, a_k \rangle$ and $y \in B = \langle b_1, \dots, b_m \rangle$.
OBJECTIVE: Find $K := x^{-1} y^{-1} x y$.

CDP (Conjugacy Decompositon Problem):
INPUT: $(s, s^x) \in G^2$ with $x \in T \subset G$.
OBJECTIVE: Find $(x_1', x_2') \in T^2$ such that $x_1' s x_2' = s^x$.

KLP (Ko-Lee Problem - a Diffie-Hellman version of the GCSP or CDP):
INPUT: $(s, s^x, s^y) \in G^3$ with $x \in A, y \in B$, and $A, B \subset G$ with $[A, B] = 1$.
OBJECTIVE: Find $K := x^{-1} y^{-1} s x y$.

DP (Decompositon Problem):
INPUT: $(s, x_1 s x_2) \in G^2$ for some $x_1, x_2 \in T \subset G$.
OBJECTIVE: Find $(x_1', x_2') \in T^2$ such that $x_1' s x_2' = x_1 s x_2$.

DH-DP (Diffie-Hellman Decompositon Problem):
INPUT: $(s, x_1 s x_2, y_1 s y_2) \in G^3$ with $x_1, x_2 \in A, y_1, y_2 \in B$, and $A, B \subset G$ with $[A, B] = 1$.
OBJECTIVE: Find $K := x_1 y_1 s x_2 y_2$.

Indeed, the AAG commutator KAP, the Ko-Lee protocol and the group DH KAP are based on the AAGP, KLP and DH-DP, respectively.
A key transport protocol based (see e.g. [**BM03**]) on the DH-DP is given in [**BC$^+$06**].
Note that the DP can be generalized by choosing x_1, x_2 from two different subgroups T_1, T_2, respectively. We call the corresponding search problem also decomposition problem. A similar remark affects the DH-DP.
Now, let P_1, P_2 be two computational problems. We say P_1 is harder than P_2 or P_1 implies P_2, written $P_1 \to P_2$, if a P_1-oracle provides a solution to problem P_2.

Proposition 5.3 *We have the following hierarchy of search problems:*

$$\begin{tikzcd}
& l\text{-SGCSP} \arrow[dl] \arrow[d] \arrow[dr] & & & \\
\text{AAGP} & l\text{-SCSP} \arrow[dr] & \text{GCSP} \arrow[d] \arrow[dr] & & \text{DP} \arrow[dl] \arrow[d] \\
& & \text{CSP} & \text{CDP} \arrow[d] & \text{DH-DP} \arrow[dl] \\
& & & \text{KLP} &
\end{tikzcd}$$

Proof. - Most of the sketched implications are obvious consequences of the definitions. We just prove CDP → KLP and l-SGCSP → AAGP:

1. The input is a triple $(s, s^x, s^y) \in G^3$ with $x \in A, y \in B$, and $A, B \subset G$ with $[A, B] = 1$. A CDP-oracle provides $(x_1, x_2) \in A^2$ with $x_1 s x_2 = s^x$. Now we can compute the shared key
$$x_1 s^y x_2 = x_1 y^{-1} s y x_2 = y^{-1}(x_1 s x_2) y = y^{-1}(x^{-1} s x) y = K.$$

2. Here the input is $\{(a_i, a_i^y) \in G^2 | i = 1, \ldots, k\} \cup \{(b_j, b_j^x) \in G^2 | j = 1, \ldots, m\}$ with $x \in A = \langle a_1, \ldots, a_k \rangle$ and $y \in B = \langle b_1, \ldots, b_m \rangle$. A m-SGCSP-oracle provides a $x' \in A$ with $x'^{-1} b_j x' = b_j^x$ for all $j = 1, \ldots, m$. And a k-SGCSP-oracle provides a $y' \in B$ with $y'^{-1} a_i y' = a_i^y$ for all $i = 1, \ldots, k$. Now, since $x'^{-1} b_j x' = b_j^x \Leftrightarrow [x' x^{-1}, b_j] = 1 \, \forall j$, we have $x' = c_b x$ for some $c_b \in C(B)$. Here $C(B)$ denotes the intersection of all

centralizers $C(b_j)$ $(j = 1, \ldots, m)$. Analogously, we can write $y' = c_a y$ with $c_a \in C(A) = \bigcap_{i=1}^k C(a_i)$.
Now, $x' \in A$ implies $c_b \in A$. Therefore we have $[c_a, c_b] = 1$, and we can compute the shared key

$$\begin{aligned} K' := x'^{-1}y'^{-1}x'y' = (c_b x)^{-1}(c_a y)^{-1} c_b x c_a y &= x^{-1}c_b^{-1}y^{-1}c_a^{-1}c_b x c_a y \\ = x^{-1}y^{-1}c_b^{-1}c_a^{-1}c_b c_a xy &\overset{!}{=} x^{-1}y^{-1}xy = K. \quad \square \end{aligned}$$

We see, that solving the classical CSP is insufficient for breaking the AAG protocol or the Ko-Lee protocol. Furthermore, it is, in general, insufficient to solve the l-SCSP to obtain the shared key K of the AAG protocol:
Let $x' = c_b x \in G$ and $y' = c_a y \in G$ with $c_a \in C(A), c_b \in C(B)$ be the output of a m-SCSP-oracle and a k-SCSP-oracle, respectively. Then we have $K' = K$ if and only if $[c_a, c_b] = 1$. A necessary condition for $[c_b, c_a] \neq 1$ is $c_b \notin A \wedge c_a \notin B$, which implies $x' \notin A \wedge y' \notin B$. Otherwise, if $x' \notin A$, but $y' \in B$ (or vice versa), the adversary gets $K' = K$.
We see that, additional to the SCSP, an adversary has to solve the

MDP (Membership Decision Problem):
Input: $x \in G$ and a subgroup $A = \langle a_1, \ldots, a_k \rangle \subset G$.
Objective: Decide whether $x \in A$ or not.

to solve the AAGP. Indeed, we have (l-SCSP $\wedge$ MDP) $\rightarrow$ l-SGCSP.
Note that the MDP is hard in most groups. For instance, the MDP is algorithmically unsolvable in $F_2 \times F_2$ [**Mi58**]. Since $F_2 \times F_2 \cong < \sigma_1^2, \sigma_2^2, \sigma_4^2, \sigma_5^2 > \subset B_6$ [**Co94**], the MDP is also algorithmically unsolvable in the braid groups for $n \geq 6$.
Alternatively, the adversary could solve the SCSP and the

MSP (Membership Search Problem):
Input: $x, a_1, \ldots, a_k \in G$.
Objective: Find an expression of x as a word in $a_1, \ldots, a_k$ (notation $x = x(a_1, \ldots, a_k)$), if it exists.

to break the AAG key agreement scheme [**SU06a**]:
If a m-SCSP-oracle outputs a $x' = c_b x \in A$, then the MSP-oracle provides the word expression $x'(a_1, \ldots, a_k)$. Now the adversary can compute the shared key

$$x'^{-1}x'(a_1^y, \ldots, a_k^y) = x'^{-1}x'^y = (x^{-1}c_b)y^{-1}(c_b x)y = [x, y] = K.$$

But we have shown above, that it is not necessary to solve the MSP.

5.2 Attacks on the braid-based key encryption schemes

In this section we describe several attacks on the braid-based cryptographic schemes introduced in the foregoing section, except of representation attacks. Representation attacks on the braid Diffie-Hellman key agreement scheme were covered in chapter 4. We add some remarks on other representation atttacks:

A linear algebra attack against the AAG scheme [**AAG99**, **AA$^+$01**] was proposed by J. Hughes in [**Hu02**], where he introduced his heuristic for inverting the Burau representation.

Further, Lee and Lee performed a linear algebra attack on the key extractor suggested in [**AA$^+$01**] (see also [**AAG06**]). Indeed, they showed that the security of the key extractor is based on the problems of listing all solutions to some SCSP's in S_n and in $GL(n-1, \mathbb{F}_p)$ (p prime) [**LL02**].

5.2.1 Solutions to the CSP and computation of centralizers and roots in braid and Garside groups

The conjugacy problem in braid groups was solved in the late sixties by Makanin [**Ma68**] and Garside [**Ga69**]. In his fundamental work Garside associated with every braid b a special finite set of conjugates of b, called the summit set of b. Then he showed that two braid are conjugated if their summit sets are identical.

Elrifai and Morton [**EM94**] improved Garside's solution to the conjugacy problem by introducing a much smaller invariant class under conjugation, the super summit set. The super summit set $SSS(b)$ of a braid b is defined as the set of all conjugates of b with minimal canonical length. An element $\tilde{b} \in SSS(b)$ can be computed by using cycling and decycling operations $\phi_+, \phi_- : B_n \to B_n$ with

$$\phi_+(b) = \Delta^p b_2 \cdots b_l \tau^{-p}(b_1) \ , \ \phi_-(b) = \Delta^p \tau^p(b_l) b_1 \cdots b_{l-1}$$

for $b = \Delta^p b_1 \cdots b_l \in G$ in LNF. Here τ denotes the flip automorphism defined by $\sigma_i \mapsto \sigma_{n-i}$. Note that cycling and decycling is nothing else than conjugating b by $\tau^{-p}(b_1)$ and b_l^{-1}, respectively. If $b \notin SSS(b)$, then, according to the Cycling Theorem [**BKL01**], one finds a conjugate b' of b with $cl(b') < cl(b)$ by cycling or decycling at most $\binom{n}{2} - 1$ times. So, by repeated cycling and/or decycling, we find a $\tilde{b} \in SSS(b)$. Starting from $\tilde{b}$, $SSS(b)$ can be computed by repeated conjugations by simple braids. Note that, by this procedure, we compute the whole directed super summit graph labeled by simple braids.

Two braids $b, \bar{b}$ are conjugated if and only if $\tilde{b} \in SSS(\bar{b})$. Now, if $b \sim \bar{b}$ (i.e. b, $\bar{b}$ are conjugated), then a conjugator can be obtained from the super summit graph of $\bar{b}$ by keeping track of the conjugating braids. This provides us with a solution to the CSP. This method was generalized by Picantin to a solution of the conjugacy problem in all Garside groups [**Pi01a**]. The first attack on a braid-based cryptosystem (the Ko-Lee protocol for B_{45}) using SSS's was published in [**Hu00**].

Franco and Gonzales-Meneses [**FG03a**] showed, that if $b^{s_1} \in SSS(b)$ and $b^{s_2} \in SSS(b)$, then $b^{s_1 \wedge s_2} \in SSS(b)$. Therefore it is sufficient to conjugate with minimal (minimal according to $\prec$) simple elements. Note that in the Artin presentation of B_n there are $n!$ simple braids, but only at most $n-1$ (the number of atoms in B_n^+) minimal simple braids. This reduces the average (vertex) degree of the super summit graph immensely. But it leads to an increase of the average minimal path length between two vertices. Further Franco and Gonzales-Meneses developed concrete algorithms to compute minimal simple elements in Garside groups [**FG03a**].

These methods were used in [**Go05**] to improve an attack on the l-SCSP by E. Lee and S. J. Lee [**LL02**]. The complexity of the algorithm used in the Lee-Lee attack is $O(N \max_i |s_i|(n!)n \log n)$ where N denotes the cardinality of the special conjugacy class

$$\begin{aligned} C^{\inf}(s_1, \ldots, s_l) &= \{(s_1', \ldots, s_l') \in B_n^l \mid \inf(s_i') \geq \inf(s_i) \quad \text{and} \\ &\qquad s_i' = x'^{-1} s_i x' \quad \text{for some} \quad x' \in B_n \forall i = 1, \ldots, l\}. \end{aligned}$$

Now, the improvement from [**Go05**] leads to an attack on the SCSP which is polynomial in n. But the complexity still depends on the cardinalty of $C^{\inf}(s_1, \ldots, s_l)$. Nevertheless the Lee-Lee attack is strong when the s_i's are short and it does not depend on how complicated the simultaneous conjugator x is. If, e.g., the s_i's are all positive, then $C^{\inf}(s_1, \ldots, s_l)$ will be very small. It was suggested in [**AA$^+$01**] to use short s_i's to prevent length attacks (see 5.2.2). Myasnikov, Shpilrain and Ushakov investigated random subgroups of B_n generated by a small number of elements $s_1, \ldots, s_l$ with $|s_i| << n$ [**MSU06**]. Their experiments showed that the parameter choice suggested in [**AA$^+$01**] is unsuitable, because "most" of these subgroups are equal to the whole group B_n. Further, "almost all" of these subgroups are generated by positive braid words, and the centralizers of these subgroups coincide with the center $\langle \Delta_n^2 \rangle$. Even with modified parameters ($n = 80, l = 20, 11 \leq |s_i| \leq 13$) many subgroups generate the whole braid group. Therefore, using the techniques from [**LL02**, **Go05**], according to [**MSU06**] it is easy to break the AAG scheme with parameters suggested in [**AA$^+$01**]. Note that Myasnikov, Shpilrain and Ushakov developed concrete algorithms how to simplify the generating sets of random subgroups of B_n [**MSU06**]. Therefore the lengths of the s_i's should be further increased, even if this contradicts with security requirements against length attacks (see 5.2.2).

A further striking improvement of the solution to the CSP is due to V. Gebhardt [**Ge05**]. Because iterated cycling in the SSS certainly becomes periodic, he showed that it is sufficient to consider a small subset of the SSS, the ultra summit set (USS), consisting of the cyclic parts of the conjugacy orbits in the SSS. He reports that for a random braid $b \in B_{100}$ with $|b| = 1000$ the $USS(b)$ can be computed efficiently (within a few seconds in his implementation). According to his experiments (and the theoretical considerations in [**BGG06b**]) it seems likely that pseudo-Anosov[2] braids have very small USS's, whereas the USS's of perodic and reducible braids may be much larger. Therefore, pseudo-Anosov braids are a very bad choice as instance braids for braid cryptosystems based on conjugacy search. But almost all long, randomly chosen braids fall into the pseudo-Anosov class.

But no polynomial bound (in n or $|b|$) is known for the size of the $USS(b)$. Indeed, according to [**BGG06c**] there are examples of periodic braids whose size of the USS is exponential in n. Particulary, we have $|USS(d^n)| = 2^{n-2}$ (Corollary 11 in [**BGG06c**]). Therefore Garside's algorithm using USS's has exponential time complexity for periodic braids. Nevertheless, using both Garside structures of braid groups a polynomial time algorithm for the conjugacy problem of periodic braids is given in [**BGG06c**]. Therefore, according to the Nielsen-Thurston trichotemy the class of reducible braids seems to remain as the only usable class of instance braids for braid cryptosystems using conjugacy search.

Further insight to the CSP was gained by Birman, Gebhardt and Gonzales-Meneses [**BGG06a**, **BGG06b**, **BGG06c**]. The authors believe that due to their increased understanding of the structure of USS's a polynomial algorithm for the CSP is within reach[3].

Before we discuss how an efficient solution to the CSP in braid groups could affect the security of the braid-based key agreement protocols, we consider the computation of centralizers and roots in B_n.

The first algorithm for computing a generating set of the centralizer $C(b)$,

[2] Since $B_n \cong \mathcal{M}(D_n)$, a braid can be, according to the Nielsen-Thurston classification of homeomorphisms [**Ni86**, **Th88a**, **Th88b**], either periodic or reducible or pseudo-Anosov.

[3] Note that P. Bangert claims, that he had found a polynomial solution to the CSP with time complexity $O(|b|^5 n^{11})$ [**Ba02a**, **Ba02b**, **Ba04**, **Ba07**]. Nevertheless his proof seems not to be well accepted in the mathematical community. One indicator are the ongoing efforts to find such a polynomial solution [**BGG06a**, **BGG06b**, **BGG06c**]. Further, according to a private communication, Gonzales-Meneses observed, that Bangert's (cyclic) term rewrite system does not recognize that σ_i and σ_j are conjugated for $i \neq j$.

$b \in B_n$, was given by Makanin [**Ma71**]. But his algorithm is very slow and provides large and highly redundant generating sets. While Makanin [**Ma71**] used simple braids, the introduction of minimal simple elements by Gonzales-Meneses and Franco [**FG03a**] leads to a much quicker algorithm for computing generating sets of centralizers, using the fact that an element in $C(b)$ is a loop in the (minimal) conjugacy graph of b [**FG02**]. In a revised version of this paper they improved their algorithm by considering the (minimal) super summit graph instead of the whole positive conjugacy graph (see section 3 in [**FG03b**]). A further improvement may come from Gebhardt's ultra summit sets.

There were several efforts to characterize the centralizers at least of special braids. Gurzo [**Gu88**] computed generators for centralizers of what he called rigid braids[4]. Fenn, Rolfsen and Zhu determined in [**FRZ96**] the centralizers of Artin generators and of naturally included braid subgroups, i.e. $C(\sigma_i)\,\forall i = 1,\ldots,n-1$ and $C(B_r)\,\forall r \leq n$. Franco and Gonzales-Meneses conjectured in [**FG02**] that the centralizer a of a braid is generated by at most $n-1$ elements. This conjecutre was disproved by Ivanov [**Iv04**], who constructed examples of centralizers with $O(n^2)$ generators. Then, using the ideas from [**Iv04**], Gonzales-Meneses and Wiest [**GW04**] proved that the generating set of the centralizer of any braid $b \in B_n$ has at most $k(k+1)/2 = n(n+2)/8$ elements if $n = 2k$, and at most $k(k+3)/2 = (n-1)(n+5)/8$ elements if $n = 2k+1$. The examples of reducible braids given in [**Iv04**] and [**GW04**] show that these bounds are sharp. In [**GW04**] the centralizers are described in terms of direct and semidirect products of mixed braid groups[5] [**Ma95**, **Or01**].

Especially, if $b \in B_n$ is pseudo-Anosov, Gonzales-Meneses and Wiest show that the centralizer is

$$C(b) = \langle \alpha \rangle \times \langle \rho \rangle \cong \mathbb{Z}^2 \cong B^2_{\{1,2\}}.$$

They describe how to compute the periodic braid ρ commuting with b. Further α is the smallest possible root of b', which is obtained from b by multiplication with a suitable power of ρ. The k-th root problem, i.e. for a given k, determining whether a given braid b has a k-th root, and computing this root, was solved in [**St78**] (translated in [**St79**]). This solution was generalized by Sibert to Garside groups in [**Si02**]. H. Zheng developed an algorithm to exract roots in Garside groups [**Zh06**] using USS's. He conjectures that this algorithm is polynomial in $|b<$. Further, Gonzales-Meneses showed that

[4] According to [**Gu88**] a braid b is called rigid if there exists exactly one positive braid word for b.

[5] The mixed braid group B_P consists of all braids b whose braid permutation $\nu(b)$ preserves a given partition P of $\{1,\ldots,n\}$.

the k-th root of a braid b is unique up to conjugacy [**Go03**]. And S. J. Lee proved that the root problem in any Garside group G can be reduced to the conjugacy problem in $\mathbb{Z} \times G^n$, which is a Garside group, too [**Le07**]. Therefore, if the conjugacy problem is effectively solvable in any Garside group, then the same holds for the root problem. Using a simple heuristic approach Groch, Hofheinz and Steinwandt developed a practical attack on the root problem in B_n [**GHS06**].

Nevertheless, for a random pseudo-Anosov braid b, an element $c \in C(b)$ usually has the form $b = b^k \Delta_n^{2l}$ for some $k, l \in \mathbb{Z}$ [**Ko01**], i.e. $\rho = \Delta_n^2$ and $\alpha = b$. Now consider the m-SCSP with input $\{(s_i, s_i^x) \in G^2 | i = 1, \ldots, m\}$ for $G = B_n$. A CSP-oracle provides solutions $x_1, \ldots, x_m$ with

$$x_1^{-1} s_1 x_1 = x^{-1} s_1 x, \ldots, x_m^{-1} s_m x_m = x^{-1} s_m x.$$

Therefore we have $x x_i^{-1} \in C(s_i)$ for all $i = 1, \ldots, m$. If the s_i's are pseudo-Anosov, then we have $x x_i^{-1} = \Delta_n^{2k_i} s_i^{l_i}$ (in general $= \rho_i^{k_i} \alpha_i^{l_i}$) for some integers k_i, l_i ($i = 1, \ldots, m$). A search for integers $k_i, l_i \in \mathbb{Z}$ ($i = 1, \ldots, m$) with

$$\Delta_n^{2k_1} s_1^{l_i} x_1 = \ldots = \Delta_n^{2k_m} s_m^{l_m} x_m =: x'$$

leads to a solution $x' \in G$ of the m-SCSP. In so far the CSP is probabilistically harder than the m-SCSP $\forall m \in \mathbb{N}$ in braid groups [**Ko01**]. Note that if the given s_i's are not all pseudo-Anosov, then we have to generalize our strategy using the results on the structure of centralizers in B_n [**GW04**]. But this doesn't lead to a solution to the m-SGCSP. Here we have to check whether the solution x' is in a given subgroup T or not, i.e. we have to solve additionally the (subgroup) MDP for T. Nevertheless we can attack the AAGP for braid groups. Consider the notation from the proof of Proposition 5.3. SCSP-oracles yield solutions $x' = c_b x \in G$ and $y' = c_a y \in G$ with $c_a \in C(A), c_b \in C(B)$. Note that we don't know how to generate elements in $C(A) = \bigcap_{i=1}^k C(a_i)$ even if we know how to generate elements in each $C(a_i)$. But the randomly chosen elements $a_1, \ldots, a_k$ are with high probability of type pseudo-Anosov. Therefore the centralizer $C(A) = \bigcap_{i=1}^k C(a_i)$ is with high probality equal to the centre $\langle \Delta_n^2 \rangle$. This implies $[c_a, c_b] = 1$ and $K' = K$. Therefore, an efficient solution to the CSP in provides a dangerous attack on the AAG KAP in braid groups.

Now, consider the GCSP with input $(s, s^x) \in G^2$ with $x \in T \subset G$ for $G = B_n$ and s of type pseudo-Anosov. A CSP-oracle provides a solution $x' \in G$ with $x'^{-1} s x' = x^{-1} s x$. This implies $x x'^{-1} \in C(s)$. Analogously, a search for $k, l \in \mathbb{Z}$ such that $\Delta_n^{2k} s^l x' \in T$ leads to a solution of the GSCP. But here we have to solve the MDP for T. For simple commuting subgroups of B_n such as LB_m, UB_{n-m}, suggested in [**KL$^+$00**], the MDP is trivial. Therefore, for

such specific subgroups, the CSP is probabilistically harder than the GCSP (and the KLP) in braid groups [**Ko01**].
Furthermore, let G be a group endowed with a solution to the CSP and with an algorithm for computing centralizers. Then N. Franco proved in [**Fr04**], that the GCSP (for the subgroup T) is solvable if there exist groups K, K' with $K' \subset K$ and a homomorphism $\phi : G \to K$, such that:

1. K' is finite,
2. $T = \phi^{-1}(K')$, and
3. there exists a solution to the MDP in K.

Gebhardt applied his practically fast method for conjugacy search in braid groups (using USS's) in [**Ge06**], where he performed an attack against the Ko-Lee problem. Using the facts that long, randomly chosen braids, i.e., braids of pseudo-Anosov type, have very small USS's and the centralizers of these braids have a very simple structure (see above [**GW04**]), he was able to recover the shared key in about 100,000 tries for 130 sets of parameter values without any failure of key recovery. Further, the average observed ratio of key recovery time to key generation time was around 6 [**Ge06**]. Therefore, the Ko-Lee protocol using randomly chosen public braids can be considered as completely broken.
A demonstration of the strength of Gebhardt's method for the AAG scheme was not explicitly performed so far. Nevertheless, we have argued above why we expect similar successful results.

Conclusion. Due to an unsuitable parameter choice [**AA$^+$01**] it is easy to find the shared key in the AAG protocol [**MSU06**].
Further, Gebhardt's practically efficient solution to the CSP in braid groups [**Ge05**] provides very dangerous attacks against the AAG and the Ko-Lee protocol. Particulary, the Ko-Lee scheme was completely broken in [**Ge06**].
A possible countermeasure is the usage of reducible braids with big USS's.
Otherwise, a solution to the CSP does not yield an attack against the (braid) group Diffie-Hellman KAP, if x and $a_l x a_r$ (and analogously x and $b_l x b_r$) are not conjugated.

5.2.2 Length attacks in B_n

Length-based attacks were suggested as possible attacks against the AAG protocol in [**AA$^+$01**] and [**HT02**], and they were studied in detail in [**GK$^+$06**].
For given elements $(b_j, x^{-1}b_j x) \in B_n^2$ $(j = 1, \ldots, m)$ we try to find the conjugator $x \in A = \langle a_1, \ldots, a_k \rangle$. We use an efficiently computable length function

$L : B_n \to \mathbb{N}$, which is required to have the property that $L(x^{-1}yx)$ is usually greater than $L(y)$ for arbitrary braids $x, y \in B_n$. Note that all naturally arising length functions seem to have this property. Now, we peel off simultaneously generator (or the inverse of a generator) by generator from the given elements $x^{-1}b_1x, \ldots, x^{-1}b_mx$. We have to fix some linear order $<$ on the set of all m-tuples of lengths. In the first step we choose a $g \in A_1 := \{a_1^{\pm 1}, \ldots, a_k^{\pm 1}\}$ for which the m-tuple

$$(L(gx^{-1}b_1xg^{-1}), \ldots, L(gx^{-1}b_mxg^{-1}))$$

is minimal with respect to the selected linear order $<$. Let $x = g_1 \cdots g_l$ with $g_i \in A_1$ be freely reduced, then g is equal to g_l with some nontrivial probablility. In this case we have $xg^{-1} = g_1 \cdots g_{l-1}$. Note, if there exist nontrivial relations between the generators $a_1, \ldots, a_m$ of A, then we try to find a g such that $l_{A_1}(xg^{-1}) < l_{A_1}(x)$. We proceed with this peeling off process until we end up with $b_1, \ldots, b_m$. This yields the conjugator x or another solution x' to the m-SCSP. In the sequel, we do not distinct between x and x'.

We can improve the length attack by using a look ahead of depth t[6]. Here, at each peeling off step, we check all products $g^{(t)} \cdots g^{(1)}$ with $g^{(i)} \in A_1$ and choose that one which yields the minimal length vector

$$(\ldots, L(g^{(t)} \cdots g^{(1)}x^{-1}b_jx(g^{(1)})^{-1} \cdots (g^{(t)})^{-1}), \ldots) \in \mathbb{N}^m$$

with respect to $<$. Alternatively we peel off just one generator $(g^{(1)})$ at each step, even if we use look ahead of depth $t > 1$. This seems to be slightly better than taking the whole word $g^{(t)} \cdots g^{(1)}$, but the differences in the computer experiments in [**GK$^+$06**] were not significant.

Empirically, for any braid b the probability that the choosen element $g \in A_1$ is a "correct" generator, i.e. the probability

$$p := Pr[L(gx^{-1}bxg^{-1}) < L(x^{-1}bx)],$$

decreases with increasing braid index n, and p increases as $|a_i|$ gets larger. Further, the probability to find the correct solution x decreases with increasing length $l_{A_1}(x)$. In order to circumvent the length attack, the authors from [**AA$^+$01**] suggested to choose "big" values for n and $l_{A_1}(x)$ and the $|a_i|$ (and $|b_j|$) should be small $\forall i = 1, \ldots, k$ ($\forall j = 1, \ldots, m$). Concrete parameter values given in [**AA$^+$01**] are $n = 80$ (or larger), $k = m = 20$, $|a_i| = |b_j| = 5-10$ and $l_{A_1}(x) = 100$.

The length functions used in [**GK$^+$06**] were the socalled Garside length and

[6] The above described procedure has a look ahead of depth 1.

the reduced Garside length function[7]. Here, the Garside length $L_G(b)$ of a braid $b \in B_n$ is the number of Artin generators needed to write b in its (Artin) Left normal form $b = \Delta_n^{-p} b_1 \cdots b_c$. And the reduced Garside length is defined as

$$L_{RG}(b) := L_G(b) - 2 \sum_{i=1}^{\min(p,c)} |b_i|.$$

It turns out that the reduced Garside length provides the best success rates to find a correct generator g [**GK$^+$06**]. Further, in [**HT06**] it is shown that the reduced BKL length[8], i.e. a BKL version of the reduced Garside length, even works better.

Nevertheless the success rates of length attacks in [**GK$^+$06**] for the parameters suggested in [**AA$^+$01**] are completely neglegible. Since the time complexity of length attacks is exponential in the look ahead parameter t, we require unfeasible computational power to break the AAG protocol.

An improvement might come from using better length functions. Note that all length functions studied in [**GK$^+$06**] and [**HT06**] come from left or mixed Garside normal forms (in the Artin or the BKL presentation). Interestingly, approximations for geodesic braids (with respect to the length $l_{\Omega_1}(\cdot)$) seem not to be used so far in (pure) length attacks. Remember that the non-minimal braid problem, i.e., given a word w in the Artin generators, decide whether there exists a word w' representing the same braid with $|w'| < |w|$, is NP-complete [**PR91**]. A good algorithm to approximate geodesic braids is the Algorithm 1 (Minimization of braids) from [**MSU05**] using Dehornoy forms, which is also used in [**MSU06**]. According to [**De04b**] the relaxation algorithm in [**Wi02**] seems, at least for small n, also to be efficient for finding short word representatives in B_n. Further, physical methods like elastic relaxation and the usage of crossing number minimizing forces are studied in [**Ba02a**], but such methods are too time consuming and they therefore apply just for sufficiently "small" braids.

The length attack seems to be specially active against the AAG KAP, because one knows several pairs of conjugate braids associated with the same conjugator [**De04b**]. Hughes and Tannenbaum [**HT02**] stated it as an interesting open question, whether the length attack may be suitably modified to be relevant to the Ko-Lee protocol. Nevertheless, according to [**GK$^+$06**] several computer experiments showed that, if we increase the number m of given braids $x^{-1}b_jx$ ($j = 1, \ldots, m$) from few (about 10) to many (about 3000), this did not yield a significantly increased probability for finding a

[7] In a preliminary draft [**GK$^+$02**] of this paper they studied additionally the socalled shortened Garside length function.

[8] Also called mixed BKL length.

"correct" generator g.
Indeed, the length attack was generalized in [**GK+05**] to a memory-based extension which provides probabilistic solutions to many combinatorial group-theoretic problems in random subgroups of B_n like the SCSP, MDP, minimal braid problem etc.

Conclusion. While the length attacks influenced the parameter choices of the AAG protocol in [**AA+01**], it is clear from [**GK+06**] that (pure) length attacks are not dangerous in practice. We propose a further investigation of short braid representatives (as used in [**MSU05**]), which could yield better length functions.

5.2.3 Hofheinz-Steinwandt attack

The Hofheinz-Steinwandt attack [**HS03**] is a practical attack on the AAG and the Ko-Lee protocol. It can be characterized as a mixture of a length-based and a projection attack. In the sequel, we follow the lucid description in [**De04b**], which explains why the Hofheinz-Steinwandt attack works so successfully.
Let b_1, b_2 be two "random" braids. We observe empirically, that for $n \geq 50$ the probability that

$$cl(b_1 b_2) = cl(b_1) + cl(b_2)$$

is practically 1, at least for $cl(b_1), cl(b_2) \leq 200$ [**De04b**]. Therefore, if b, c are random braids, we have with probability close to 1

$$cl(c^{-1}bc) = cl(b) + 2cl(c),$$

i.e., the canonical length of a random conjugate of b is higher than that of b. This seems to be paradoxical, since conjugacy is a symmetric relation, but it just depends on the way the conjugates are chosen.
Now, consider $b, b' = c^{-1}bc$ as instance braids of the conjugacy search problem. b lies with overwhelming probability in its super summit set $SSS(b)$[9] and we have $cl(b') > cl(b)$. In the Hofheinz-Steinwandt approach we perform, starting with b', cyclings and/or decyclings until we reach an element $\tilde{b}'$ with $cl(\tilde{b}') = cl(b)$, i.e. $\tilde{b}' \in SSS(b)$. Now Hofheinz and Steinwandt conjecture that it is probable that $\tilde{b}'$ and b are simply conjugated. The plausibility of this conjecture is established by the considerations above. Since the simple elements of the Artin presentation are permutation braids, this conjectured

[9] This is true for the parameters suggested for the braid-based KAPs.

simple conjugator can be determined by an projection attack[10] using the natural projection of B_n onto S_n. Now we just have to solve the CSP in the symmetric group for the instance pair $(\nu(b), \nu(\tilde{b}'))$.
Though we have to find in the case of the Ko-Lee KAP a conjugator within a proper subgroup of B_n, this seemingly simple mixture of a cycling and projection attack breaks the Ko-Lee protocol with a success rate of 80% for $n = 90$ and $cl(b) = cl(c) = 12$ usually within a few seconds.
A straightforward generalization of this approach which applies to the simultaneous CSP (Algorithm B in [**HS03**]) breaks the AAG protocol with a success rate of 99% for the parameters suggested in [**AA$^+$01**]. Further Hofheinz and Steinwandt develop improvements of their attack in order to deal with pure braids as instance braids[**HS03**], which was suggested in [**KL$^+$00**] and [**LL02**] for the Ko-Lee and the AAG protocol[11], respectively.
Dehornoy points out, that the effectivity of the Hofheinz-Steinwandt attack relies on way the keys are chosen [**De04b**]. Given $b \in SSS(b)$, if we choose c such that $c^{-1}bc$ is also in $SSS(b)$ and the distance between b and $c^{-1}bc$ in the super summit graph (called "permutation distance" in [**De04b**]) is large (at least 2), then this countermeasure prevents the Hofheinz-Steinwandt attack. Note that in the AAG scheme we have to find a conjugator a for given elements $b_1, \ldots, b_m$ such that the "permutation distance" is simultaneously large for all pairs $(b_j, a^{-1}b_ja)$. Therefore it seems to be much more difficult to find secure instances of the AAG protocol. Nevertheless, the elements $s_1, \ldots, s_m$ and $t_1, \ldots, t_n$ should lie in their super summit sets.
It would be interesting to apply the Hofheinz-Steinwandt attack in the dual (BKL) presentation. In this case, if $b, \tilde{b}' \in SSS^{\text{dual}}(b)$ are simply conjugated[12] then we have to find a solution to the CSP in S_n for the instance pair $(b, \tilde{b}')$, restricted to permutations which describe non-crossing partitions. Note that the CSP in symmetric groups is easy, but there are in general many solutions. Such a dual Hofheinz-Steinwandt attack leads to the additional requirement, that b and $c^{-1}bc$ should be both in $SSS^{\text{dual}}(b)$, and their distance in the dual super summit graph should be also sufficiently large.

[10] Notice that, in general, projection attacks alone are not successful against computational problems, because it turns out to be difficult to recover the lost information. Projection attacks are usually used against decision problems. An example in the field of braid-based cryptography is the attack given in [**GM02**].

[11] Note that the conjugacy decision problem for subgroups of the pure braid group P_n is unsolvable for $n \geq 5$ [**BD99**], i.e. there exists no (deterministic) algorithm that allows one to decide whether two given finitely generated subgroups are conjugate in P_5 or not. Nevertheless, this does not affect the AAG scheme, since the given subgroups $\langle s_1, \ldots, s_l \rangle$ and $a^{-1}\langle s_1, \ldots, s_l \rangle a$ are known to be conjugated.

[12] Of course, this $\tilde{b}'$ differs from that obtained by using cyclings/decyclings in the Artin presentation.

S. Maffre developed an approach to the conjugacy search problem which is related to the Hofheinz-Steinwandt attack. While the cycling attack of Hofheinz and Steinwandt allows us to determine a prefix (left divisor) d of the secret a, i.e. $d \prec a$, Maffre proposed an algorithm which computes a prefix ($d \prec a$) and a multiple of the secret ($m \succ a$) [**Ma06a**, **Ma06b**]. This can be used to reduce the Artin length of the secret. Further, we can reduce the CSP-instance $(x, a^{-1}xa)$ to the two reducts $(x, da^{-1}xad^{-1})$ and $(x, ma^{-1}xam^{-1})$. Maffre used this reduction to test weak keys of the proposed cryptographic primitives based on variants of the CSP [**Ma06a**, **Ma06b**].

Conclusion. The Hofheinz-Steinwandt attack breaks the AAG and the Ko-Lee protocol effectively. At least in the case of the Ko-Lee protocol, we can avoid this attack by using proper instance braids. The Hofheinz-Steinwandt attack (and the work of Maffre) do not affect to the braid Diffie-Hellman KAP.

5.2.4 Practical attack on the braid Diffie-Hellman key exchange

At the CRYPTO 2005 Myasnikov, Shpilrain and Ushakov presented a practical heuristic solving the decompostion problem (DP) in braid groups with success rates over 95%. This implies an attack against the braid Diffie-Hellman key exchange (and also against the Ko-Lee protocol). In this attack geodesic braids are approximated by an algorithm extensively using Dehornoy forms. Therefore we begin with a short description of Dehornoy's handle reduction algorithm. Consider a left (or lower) σ_i-handle, i.e. a braid word of the form

$$w = \sigma_i^{\epsilon} w_0 (\sigma_{i+1}^{\zeta_1} w_1) \cdots (\sigma_{i+1}^{\zeta_k} w_k) \sigma_i^{-\epsilon}$$

with $\epsilon, \zeta_1, \ldots, \zeta_k \in \{\pm 1\}$, $w_0, w_1, \ldots, w_k \in \langle \sigma_{i+2}, \ldots, \sigma_{n-1} \rangle$[13] and $k \geq 0$. Such a σ_i-handle is reduced to the word

$$w' = w_0 (\sigma_{i+1}^{-\epsilon} \sigma_i^{\zeta_1} \sigma_{i+1}^{\epsilon} w_1) \cdots (\sigma_{i+1}^{-\epsilon} \sigma_i^{\zeta_k} \sigma_{i+1}^{\epsilon} w_k),$$

which is equivalent to w, i.e. it represents the same braid. For $k = 0$ and $w_0 = e$ we get $w = \sigma_i^{\epsilon} \sigma_i^{-\epsilon}$ and $w' = e$. Therefore free reduction is a special case of handle reduction. Dehornoy proved that every handle reduction sequence starting with w stops after at most $2^{n|w|^4}$ steps at an irreducible

[13] For a straightforward generalization of a σ_i-handle the w_j's lie in $\langle \sigma_1, \ldots, \sigma_{i-2} \rangle \cdot \langle \sigma_{i+2}, \ldots, \sigma_{n-1} \rangle$.

word [**De97**]. Further, there are no representatives of the trivial braid with word length > 0. Therefore, if we fix a strategy determining in which order the handles have to be reduced, Dehornoy's handle reduction algorithm provides a solution to the word problem in B_n. We refer to the irreducible word obtained from a handle reduction sequence applied to a braid word w as Dehornoy form $D(w)$.

While the above mentioned upper bound for the complexity of Dehornoy's algorithm is exponetial in n and $|w|$, it turns out that handle reduction is extremely efficient in practice, i.e. for random braids. For big n, it outperforms even the Garside normal forms (complexity $O(|w|^2 n \log n)$).

The word length of the Dehornoy form $D(w)$ of a random braid word w (representing a braid $b \in B_n$) is according to table 3.2 in [**DD$^+$02**] usually greater than $|w|$ for $n| \leq 64$ and $|w| \leq 4096$. But for the cryptographic relevant parameter values used in [**MSU05**] ($n = 100$ and $|w| = 2000$ or 4000) we usually have $|D(w)| < |w|$. The minimization algorithm $Shorten(w)$ in [**MSU05**] uses (left) handle reduction to remove all left handles. This might introduce right (or upper) handles. Now, if $|D(w)| < |w|$, we apply right handle reduction to remove all right handles and so on. We use alternately left and right handle reduction until the word length of a (left or right) Dehornoy form is greater or equal than the word length of the actual input word. The word obtained by this shortening process is assumed to be a good approximate for a geodesic braid word. According to [**MSU05**] it is questionable whether there exist Dehornoy forms without both left and right handles.

Now, given $x, y \in B_n$ with $y = a_l x a_r$ for some $a_l, a_r \in LB_m$, the practical attack on the decomposition problem developed in [**MSU05**] works roughly as follows.

1. Let w_1, w_2 be words representing the instance braids x, y, respectively. First we simplify the instance pair (w_1, w_2) to (s_1, s_2) in three steps.

   (a) Find shorter braid representatives than w_1, w_2 using the above mentioned algorithm. The reduced words are $w_1' = Shorten(w_1)$ and $w_2' = Shorten(w_2)$.

   (b) Find a decomposition $(l_i, t_i, r_i) \in LB_m \times B_n \times LB_m$ of w_i' with $w_i' = l_i t_i r_i$ and $|t_i| < |w_i'|$ for $i = 1, 2$. Algorithm 3 in [**MSU05**], which extensively uses Dehornoy forms, tries to make t_1, t_2 as short as possible.

   (c) Find braid words $u, v \in UB_{n-m}$ and $s_1, s_2 \in B_n$ with $|s_1| < |t_1|$ such that $us_1v = t_1$ and $us_2v = t_2$. Algorithm 4 in [**MSU05**], also extensively using Dehornoy forms, tries to make s_1, s_2 as short as possible.

The pair of braid words (s_1, s_2) is called a simplified pair of (w_1, w_2). Let

$$S_{(w_1,w_2)} = \{(a'_l, a'_r) \in LB_m^2 \mid a'_l w_1 a'_r = w_2\} = S_{(w'_1,w'_2)}$$

be the set of solutions for the DP for the instance pair (w_1, w_2). Then we have

$$\begin{aligned} & (q_l, q_r) \in S_{(s_1,s_2)} \quad \Leftrightarrow \quad q_l s_1 q_r = s_2 \quad \Leftrightarrow \quad q_l u^{-1} t_1 v^{-1} q_r = u^{-1} t_2 v^{-1} \\ \Leftrightarrow \quad & q_l t_1 q_r = t_2 \quad \Leftrightarrow \quad q_l l_1^{-1} w_1 r_1^{-1} q_r = l_2^{-1} w_2 r_2^{-1} \\ \Leftrightarrow \quad & (l_2 q_l l_1^{-1}, r_1^{-1} q_r r_2) \in S_{(w_1,w_2)}. \end{aligned}$$

2. Solve the DP for the simplified pair (s_1, s_2).
Here we perform a heuristic search in the set of all pairs of braid words, representing braids in LB_m. This set is represented as a digraph whose edge set E contains edges of the following two types:

   - If $q_l = q'_l$ and $q'_r = q_r^{(1)} \sigma_j^{\epsilon} q_r^{(2)}$ where $q_r = q_r^{(1)} q_r^{(2)}$, $j \in \{1 \ldots, n-1\}$ and $\epsilon \in \{\pm 1\}$, then $((q_l, q_r), (q'_l, q'_r)) \in E$.
   - If $q_r = q'_r$ and $q'_l = q_l^{(1)} \sigma_j^{\epsilon} q_l^{(2)}$ where $q_l = q_l^{(1)} q_l^{(2)}$, $j \in \{1 \ldots, n-1\}$ and $\epsilon \in \{\pm 1\}$, then $((q_l, q_r), (q'_l, q'_r)) \in E$.

   Let $CycShorten(\cdot)$ be a straightforward generalization of the minimizing algorithm $Shorten(\cdot)$ for cyclic braid words, then we define by

$$\omega(q_l, q_r) := |CycShorten(q_l s_1 q_r s_2^{-1})|$$

   a length function on the set of all pairs of braid words. Solutions to the DP-instance (s_1, s_2) obviously satisfy $\omega(q_l, q_r) = 0$. Therefore the heuristic search, starting at (e, e), tries to minimize the length function ω.

   A. Initialize $Q := \{(e, e)\}$.

   B. Select an unchecked pair (q_l, q_r) from Q with minimal ω-value.

   C. If $((q_l, q_r), (q'_l, q'_r)) \in E$ then add (q'_l, q'_r) to Q.
   If $\omega(q'_l, q'_r) = 0$ then return $(l_2 q'_l l_1^{-1}, r_1^{-1} q'_r r_2)$ else goto A.

In the experiments in [**MSU05**] $x \in B_n, a_l, a_r \in LB_m$ are chosen as random braid words with $n = 100$, $m = n/2$, $|x| = 2000$ and $|a_l| = |a_r| = 1000$. $y = a_l x a_r$ is given in a rewritten form (Garside normal form) ξ and therefore ξ has to be converted in a braid word w_2 before we apply the attack. Note that x, a_l and a_r are chosen in [**KL$^+$00**] and [**CK$^+$01**] as products of p canonical factors. Typical parameters used in [**KL$^+$00**] are $n = 90$ and

$p = 12$[14]. Now, the canonical length of a random braid word (representing a braid in B_n) of length l is approximately $\frac{3l}{2n}$ for sufficiently great l. This implies that the instances cracked in [**MSU05**] are even harder than the one considered in [**KL$^+$00**], but they are not harder than the one suggested in [**CK$^+$01**].
Nevertheless, for the above parameter values the heuristic attack from Myasnikov, Shpilrain and Ushakov breaks the braid Diffie-Hellman protocol with a success rate of 96% within a running time of 150 minutes on a computer cluster of 8 PC's with 2 GHz processor and 1GB memory each [**MSU05**].
Despite of increasing parameters (as in [**CK$^+$01**]) which obviously contradicts with efficiency requirements, Myasnikov, Shpilrain and Ushakov suggest to choose the word w_1 for x as a geodesic in the Cayley graph of B_n such that any geodesic representing x starts and terminates with σ_m or σ_m^{-1}. The simplified pair of (w_1, w_2) for such a word w_1 and any other braid word w_2 is also (w_1, w_2), i.e. there is no simplification.

Conclusion. The heuristic attack from Myasnikov, Shpilrain and Ushakov [**MSU05**] breaks the braid Diffie-Hellman key exchange effectively and efficiently on a computer cluster. It would be interesting to investigate whether this heuristic search works successfully for simplified or unsimplifiable instance pairs.

5.3 Further key exchange protocol based on the decomposition problem

In [**SU06b**] V. Shpilrain and A. Ushakov proposed an improved version of the group Diffie-Hellman key agreement scheme. Let x be a public element in the platform group G. Then Alice and Bob have to perform the following protocol steps:

1.A. Alice selects an element $a_l \in G$, computes a subgroup L of the centralizer $C(a_l)$, and publishes the generators $l_1, \ldots, l_k$ of L.

1.B. Bob chooses an element $b_r \in G$, selects a subgroup $R \subset C(b_r)$, and publishes the generators $r_1, \ldots, r_m$ of R.

2.A. Alice chooses a random element $a_r \in R = \langle r_1, \ldots, r_m \rangle$ and sends $y_A = a_l x a_r$ in a rewritten form to Bob.

[14] The parameters used in [**CK$^+$01**] vary from $(n, p) = (150, 15)$ to $(250, 40)$

2.B. Analogeously, Bob chooses a random element $b_l \in L = \langle l_1, \ldots, l_k \rangle$ and sends $y_B = b_l x b_r$ in a rewritten form to Alice.

3.A. Alice receives y_B and computes $K := a_l y_B a_r$.

3.B. Bob receives y_A and computes $K' := b_l y_A b_r$.

Since $b_l \in L \subset C(a_l)$ and $a_r \in R \subset C(b_r)$, we have $[a_l, b_l] = 1 = [a_r, b_r]$ which implies $K' = K$.

If an attacker wants to obtain Alice's private key, then he has to solve the following

Base Problem:
INPUT: Two subgroups $L = \langle l_1, \ldots, l_k \rangle$, $R = \langle r_1, \ldots, r_m \rangle$ of G and two elements x, y_A with $y_A = a_l x a_r \in G$ for some $a_1 \in C(L)$, $a_r \in R$.
OBJECTIVE: Find $a'_1 \in C(L)$ and $a'_r \in R$ such that $a'_l x a'_r = y_A$.

The authors of **[SU06b]** refer to this problem as a search version of the membership problem in the double coset $C(L) \cdot x \cdot R$. In our terminology it is a (generalized) decomposition problem (DP) with subgroups $T_1 = C(L)$ and $T_2 = R$. Note that in order to solve the DP, an attacker always has to face a subgroup membership problem. But in the case of the original braid Diffie-Hellman KAP the membership problem for the subgroups LB_m and UB_{n-m} is trivial. Here the membership decision problems for the subgroups $C(L)$ and R are much more difficult. Further, the attacker has to compute the centralizer $C(L)$ before he can face this DP. Therefore, this Shpilrain-Ushakov KAP seems to be much harder to break than the original braid Diffie-Hellman KAP.
Shpilrain and Ushakov propose braid groups as platform groups for their key establishment protocol. Further, they present techniques how one can efficiently generate commuting elements in braid groups

5.4 Further cryptographic primitives

Key establishment and public key cryptosystems for encyphering-deciphering are not the only cryptographic primtives using braid groups. Since the invention of braid-based cryptography other cryptographic protocols using braid groups like signature and authentication schemes were introduced. They are mentioned in the next two subsections.
Also a pseudorandom number generator and synthesizer based on the decional version of the socalled Ko-Lee assumption were suggested in **[LLH01]**.

But it was proved in [**GM02**] that the decisional Ko-Lee assumption for braid groups is false.
Further, hash functions $h : B_n \to \{0,1\}^*$, which are used in several braid-based schemes, are discussed in section 4.4 of [**De04b**].

5.4.1 Signature schemes

The first signature schemes based on braid groups were proposed by Ko, Choi, Cho and Lee [**KC$^+$02**]. We describe their braid signature scheme (BSS) for general platform groups G. Let $H : \{0,1\}^* \to G$ be an one-way hash function.

Key generation The secret key is an element $s \in G$ and the public key is a CSP-hard pair $(x, x') \in G^2$ with $x' = s^{-1}xs$.

Signing Given a message m, select a random $r \in G$, and let $y = H(m||\alpha)$ with $\alpha = r^{-1}xr$. Now, the signature is $\sigma = (\alpha, \beta, \gamma)$ with $\beta = r^{-1}yr$ and $\gamma = r^{-1}sys^{-1}r$.

Verifying A signature is valid iff $\alpha \sim x$, $\beta \sim \gamma \sim y$, $\alpha\beta \sim xy$ and $\alpha\gamma \sim x'y$.

The BSS is obviously based on the

MTSP (Matching Triple Search Problem):
INPUT: CSP-hard pair $(x, x') \in G^2$ and a $y \in G$.
OBJECTIVE: Find a triple $(\alpha, \beta, \gamma) \in G^3$ such that $\alpha \sim x$, $\beta \sim \gamma \sim y$, $\alpha\beta \sim xy$ and $\alpha\gamma \sim x'y$.

A closely related search problem is the

MCSP (Matching Conjugacy Search Problem):
INPUT: CSP-hard pair $(x, x') \in G^2$ and a $y \in G$.
OBJECTIVE: Find an element $y' \in G$ such that $y \sim y'$ and $xy \sim x'y'$.

Proposition 5.4 (Section 2.2 in [**KC$^+$02**]) *The CSP is harder than the MCSP and the MTSP.*

PROOF. - A CSP-oracle provides a solution s' to the CSP-instance (x, x'), i.e. $x' = s'^{-1}xs'$. Now, $y' := s'^{-1}ys'$ is a solution to the MCSP, because $y' \sim y$ and $x'y' = (s'^{-1}xs')(s'^{-1}ys') = (xy)^{s'} \sim xy$.
Further, choose an arbitrary $r' \in G$, then

$$(\alpha, \beta, \gamma) = (r'^{-1}xr', r'^{-1}yr', r'^{-1}s'ys'^{-1}r')$$

solves the MTSP, because $\alpha = x^{r'} \sim x$, $\beta = y^{r'} \sim y$, $\alpha\beta = (xy)^{r'} \sim xy$, $\gamma = y^{s'^{-1}r'}$ and $\alpha\gamma = (x'y)^{s'^{-1}r'}$. □

Proposition 5.5 (Section 2.2 in [**KC**$^{+}$**02**]) *MCSP is feasible iff and only if MTSP is feasible.*

PROOF. - 1) MCSP → MTSP: Let γ be a solution to the MCSP-instance (x', α) and y, i.e. $y \sim \gamma$ and $x'y \sim \alpha\gamma$. Then (α, β, γ) with $\alpha = r'^{-1}xr'$ and $\beta = r'^{-1}yr'$ for any arbitrary $r' \in G$ solves the MTSP.

2) MTSP → MCSP: For instance (x, x') and y a MTSP-oracle provides a solution (α, β, γ), i.e. $\alpha \sim x$, $\beta \sim \gamma \sim y$, $\alpha\beta \sim xy$ and $\alpha\gamma \sim x'y$. Therefore β is a solution to the MCSP-instance (x, α) and y, and γ is a solution to the MCSP-instance (x', α) and y. This implies that (x, α) and (x', α) are not CSP-hard pairs. Hence (x, x') is not CSP-hard and the MCSP is feasible. □

Platform groups for the BSS are all non-commutative groups with a gap between the search and the decision version of the conjugacy problem. The CSP must be hard, but the conjugacy decision problem should be feasible in order to verify the signature efficiently. In the case of braid groups the authors of [**KC**$^{+}$**02**] propose a conjugacy decision algorithm using Alexander polynomial test etc., which solves the conjugacy decision problem with overwhelming probability.
Gebhardt's practically efficient solution to the CSP in braid groups [**Ge05**] seems to provide a dangerous attack against the BSS. Therefore the braids x, x' should have big USS's in order to provide a CSP-hard instance pair.
Undeniable signature schemes[15] using braid group are proposed by Thomas and Lal in [**TL06a**]. The simple undeniable signature scheme (section 4 in [**TL06a**]) is based on a simultaneos decomposition problem (SDP), while the zeroknowledge undeniable signature scheme (section 5 in [**TL06a**]) relies on the SCSP.
Thomas and Lal also proposed three group signature schemes[16] using the CSP, SCSP, DP, a simultaneous DP and the root problem in braid groups

[15] The concept of undeniable signature scheme was introduced 1989 by Chaum and van Antwerpen [**CA90**] for limiting the ability of a third party to verify the validity of a signature.

[16] Group signature schemes were introduced 1991 by Chaum and van Heyst [**CH91**]. They are generalizations of credential mechanisms [**Ch86**] and membership authentification schemes [**SKI90**, **OOK91**], where a group member convinces a verifier that he belongs to a certain group without revealing his identity. With group signature schemes the group member can sign messages on behalf of the group.

[**TL06b**].
Further a designated verifier group signature scheme[17] based on the Ko-Lee problem and the root problem in braid groups was introduced in [**ZZQ06**].

5.4.2 Authentication schemes

The first three braid-based authentication (or identification) schemes were proposed in 2002 by Sibert, Dehornoy and Girault [**SDG06**]. Their Scheme I (section 3.1 in [**SDG06**]) is a Diffie-Hellman-like authentication scheme based on the Ko-Lee problem. We describe a slightly generalized version based on the DH-DP.
Let Alice be the prover and Bob the verifier. Alice's secret key is a pair $(a_l, a_r) \in LB_m^2$ and her public key is a pair $(x, y_A) \in B_n^2$ with $y_A = a_l x a_r$. Further $h : B_n \to \{0,1\}^*$ is a collisionfree one-way hash function on B_n. The protocol steps are:

1. Bob chooses random braids $(b_l, b_r) \in UB_{n-m}$, and he sends the challenge $y_B = b_l x b_r$.

2. Alice transmits the response $r = h(a_l y_B a_r)$, and Bob checks $r \overset{?}{=} h(b_l y_A b_r)$.

Another two-pass protocol is scheme I in [**LC05**]. But this scheme is not based on the root problem as proposed by the authors. This scheme can be broken immediately as it was shown by B. Tsaban [**Ts05**].
Further scheme II from [**LC05**] turns out to be a special case of the above described DH-DP-based scheme. Therefore, we just have to specify $a_l = a^e, a_r = a^f, b_l = b^e, b_r = b^f$ for some $a \in LB_m, b \in UB_{n-m}$ and $e, f \geq 2$. We see, that scheme II from [**LC05**] is also based on the DH-DP.
The authentication schemes II and III from [**SDG06**] are reminiscent of the famous Fiat-Shamir zero-knowledge protocol [**FS87**, **FFS88**]. While scheme II is based on the CSP, scheme III is based on the CSP or on the root (finding) problem. We describe scheme II from [**SDG06**] for general groups G. Alice's (the prover) secret key is an element $s \in G$, and her public key consists of a conjugate pair $(x, x') \in G^2$ such that $x' = s^{-1}xs$. Now, Alice and Bob repeats $k \in \mathbb{N}$ times the following three-pass protocol.

1. Alice selects a random element $r \in S$, and she sends the commitment $c = r^{-1}xr$ to Bob.

[17] The concept of a designated verifier group signature scheme was introduced 1996 by Jakobssson, Sako and Impagliazzo [**JSI96**]. Here a signature can only be verified by a single designated verifier chosen by the signer. The designated verifier can check whether the signer is a member of the group, but he cannot identify the signer.

2. Bob chooses a random bit $b \in \{0,1\}$ and transmits it to Alice.

3.0 If $b = 0$, then Alice sends $r_0 = r$, and Bob checks $c \stackrel{?}{=} r_0^{-1} x r_0$.

3.1 If $b = 1$, then Alice sends $r_1 = s^{-1} r$, and Bob checks $c \stackrel{?}{=} r_1^{-1} x r_1$.

While the verification for $b = 0$ is obvious, in the case $b = 1$ Bob verifies Alice's secret because of

$$r_1^{-1} x r_1 = (r^{-1} s) s^{-1} x s (s^{-1} r) = r^{-1} x r = c.$$

Note that the usual way, known from key agreement protocols [**AAG99**, **KL$^+$00**], how to generate CSP-instance pairs (x, x') works as follows: Generate x, choose a random s, and define $x' = s^{-1} x s$. But this approach is vulnerable to length attacks, because often there exists a length function L on G, like canonical length in braid groups etc., which satisfy $L(x) < L(s^{-1} x s)$ [**De04b**].
In order to avoid length attacks, Dehornoy points out that there exists a better choice of a CSP-instance pair (x, x') [**De05**]: Choose secret elements $x_0, s, s' \in G$, and then set $x = s^{-1} x_0 s$ and $x' = s'^{-1} x_0 s'$.
In the case of braid groups, s, s' should have the same canonical length. But there are two Garside structures on B_n, and therefore also two canonical length functions. In general, you cannot avoid all length attacks by choosing s, s' in such a way, that $L(s) \approx L(s')$ for all length functions on G.
Nevertheless, Sibert (2003) [**De05**] used this idea to develop a "bit-symmetric" version of the authentication scheme II from [**SDG06**]:
Now, $(x_0, s, s') \in G^3$ is Alice's private key, and $(x, x') \in G^2$ with $x = s^{-1} x_0 s$ and $x' = s'^{-1} x_0 s'$ is her public key. We describe a three-pass protocol round.

1. Alice selects a random element $r \in S$, and she sends the commitment $c = r^{-1} x_0 r$ to Bob.

2. Bob chooses a random bit $b \in \{0,1\}$ and transmits it to Alice.

3.0 If $b = 0$, then Alice sends $r_0 = s^{-1} r$, and Bob checks $c \stackrel{?}{=} r_0^{-1} x r_0$.

3.1 If $b = 1$, then Alice sends $r_1 = s'^{-1} r$, and Bob checks $c \stackrel{?}{=} r_1^{-1} x' r_1$.

The verification of Alice's secret succeeds in both cases, because

$$\begin{aligned} b = 0: &\qquad r_0^{-1} x r_0 = (r^{-1} s) s^{-1} x_0 s (s^{-1} r) = r^{-1} x_0 r = c, \\ b = 1: &\qquad r_1^{-1} x r_1 = (r^{-1} s') s'^{-1} x_0 s' (s'^{-1} r) = r^{-1} x_0 r = c. \end{aligned}$$

We emphasize that Dehornoy's suggestion for constructing CSP-instances (x, x') with $L(x) \approx L(x')$ for some length function L [**De05**] obviously apply to authentication schemes, because here only the prover constructs the CSP-instance. In the case of key establishment the CSP-instances are constructed by Alice and Bob, sometimes entangled in a nontrivial manner. It seems that Dehornoy's suggestion does not apply to the known group-based KAPs. We leave it as an open question, dedicated to future work.

Further, the first provably-secure authentication scheme based on braid groups, introduced by Z. Kim (Scheme I in [**Ki04**], see also [**KK04**]) and using ideas from [**KC$^+$02**], is also a Fiat-Shamir-like scheme, and it relies on the MTSP. Since scheme I from [**SDG06**] is based on the DH-DP, it can be attacked effectively by the Myasnikov-Shpilrain-Ushakov attack [**MSU05**]. Scheme II from [**SDG06**] and the Z. Kim's scheme can be attacked by Gebhardt's practically efficient solution to the CSP in braid groups [**Ge05**]. In order to prevent this attack, it is necessary to use CSP-hard instances with big USS's. Scheme III from [**SDG06**] was broken in [**GHS06**].

Special attention deserves a Fiat-Shamir-like authentification scheme using shifted conjugacy by Dehornoy [**De06**]. We describe this scheme in chapter 6.

Chapter 6

Shifted conjugacy in braid-based cryptography

6.1 Examples for LD-systems

Definition 6.1 *An* LD-system $(S, *)$ *is a set* S *equipped with a binary operation* $*$ *on* S *which satisfies the* left self-distributivity *law*

$$x * (y * z) = (x * y) * (x * z) \quad \forall x, y, z \in S.$$

Analogously, RD-systems *fulfill* $(x * y) * z = (x * z) * (y * z)$ *for all* $x, y, z \in S$.

We list some examples of LD-systems taken from [**De06**].

1. We begin with a trivial example. $(S, *)$ with $x * y = f(y)$ is an LD-system for any function $f : S \to S$.

2. A set S with a binary operation $*$, that satisfies no other relations than those resulting from the left self-distributivity law, is a free LD-system. Free LD-systems are studied extensively in [**De00**].

3. A classical example of an LD-system is $(G, *)$ where G is a group equipped with the conjugacy operation $x * y = x^{-1}yx$ or $x * y = xyx^{-1}$. Note that such an LD-system cannot be free, because conjugacy satisfies additionaly the idempotency law $x * x = x$.

4. Finite groups equipped with the conjugacy operation are not the only finite LD-systems. Indeed, the socalled Laver tables provide the classical example for finite LD-systems. There exists for each $n \in \mathbb{N}$ an unique LD-system $L_n = (\mathbb{Z}/2^n\mathbb{Z}, *)$ with $k * 1 = k + 1$. The values for $k * l$ with $l \neq 1$

can be computed by induction using the left self-distributive law. The Laver tables for $n = 1, 2, 3$ are

L_1	1	0
1	0	0
0	1	0

L_2	1	2	3	0
1	2	0	2	0
2	3	0	3	0
3	0	0	0	0
0	1	2	3	0

L_3	1	2	3	4	5	6	7	0
1	2	4	6	0	2	4	6	0
2	3	4	7	0	3	4	7	0
3	4	0	4	0	4	0	4	0
4	5	6	7	0	5	6	7	0
5	6	0	6	0	6	0	6	0
6	7	0	7	0	7	0	7	0
7	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	0

Laver tables are also described in [**De00**].

5. Consider the following braid group with infintely many strands:

$$B_{\mathbb{N}} = \left\langle \sigma_1, \sigma_2, \ldots \;\middle|\; \begin{array}{c} \sigma_i\sigma_j = \sigma_j\sigma_i \quad \forall i, j \in \mathbb{N} : \ |i-j| \geq 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \quad \forall i \in \mathbb{N} \end{array} \right\rangle.$$

The shift mapping $\mathrm{sh} : B_{\mathbb{N}} \to B_{\mathbb{N}}$ defined by $\sigma_i \mapsto \sigma_{i+1}$ is an injective homomorphism.

Proposition 6.2 *$B_{\mathbb{N}}$ equipped with the* shifted conjugacy *operation*

$$x * y = \mathrm{sh}x^{-1} \cdot \sigma_1 \cdot \mathrm{sh}y \cdot x$$

is an LD-system.

Proof. - This is a simple verification using $[\sigma_1, \mathrm{sh}^2 x] = 1$ for all $x \in B_{\mathbb{N}}$:

$$\begin{aligned} & x * (y * z) = x * (\mathrm{sh}y^{-1} \cdot \sigma_1 \mathrm{sh}z \cdot y) = \mathrm{sh}x^{-1} \cdot \sigma_1(\mathrm{sh}^2 y^{-1} \cdot \sigma_2 \mathrm{sh}^2 z \cdot \mathrm{sh}y)x. \\ & (x * y) * (x * z) = (\mathrm{sh}x^{-1} \cdot \sigma_1 \mathrm{sh}y \cdot x) * (\mathrm{sh}x^{-1} \cdot \sigma_1 \mathrm{sh}z \cdot x) \\ = \ & (\mathrm{sh}x^{-1} \cdot \mathrm{sh}^2 y^{-1} \cdot \sigma_2^{-1} \mathrm{sh}^2 x)\sigma_1(\mathrm{sh}^2 x^{-1} \cdot \sigma_2 \mathrm{sh}^2 z \cdot \mathrm{sh}x)(\mathrm{sh}x^{-1} \cdot \sigma_1 \mathrm{sh}y \cdot x) \\ = \ & \mathrm{sh}x^{-1} \cdot \mathrm{sh}^2 y^{-1} \cdot \sigma_2^{-1}\sigma_1\sigma_2\sigma_1 \mathrm{sh}^2 z \cdot \mathrm{sh}y \cdot x = x * (y * z). \end{aligned}$$

The last equality holds since $\sigma_2^{-1}\sigma_1\sigma_2\sigma_1 = \sigma_1\sigma_2$. □

Obviously, "reverse" shifted conjugacy defined by $x \bar{*} y = x\mathrm{sh}y \cdot \sigma_1 \mathrm{sh}x^{-1}$ also provides an LD-structure on $B_{\mathbb{N}}$.
It is shown in [**De94**, **De00**] that every braid generates under $*$ a free sub-LD-system of $(B_{\mathbb{N}}, *)$. But $(B_{\mathbb{N}}, *)$ is not a free LD-system. Indeed, it is even

conjectured that $(B_{\mathbb{N}}, *)$ contains no free LD-systems with two generators. Shifted conjugacy differs immensly from usual conjugacy in the braid groups. For example, the exponent sum es is not a shifted conjugacy invariant. Indeed, we have $es(x * y) = 1 + es(y)$. As a trivial consequence, there exists no element $\epsilon \in B_{\mathbb{N}}$ such that $\epsilon * x = x$ for some $x \in B_{\mathbb{N}}$. Further, if $x' = c * x$, then there exists no $\bar{c} \in B_{\mathbb{N}}$ with $x = \bar{c} * x'$. And if $x'' = c' * x'$ and $x' = c * x$ hold, then there exists no $\bar{c} \in B_{\mathbb{N}}$ with $x'' = \bar{c} * x$. In particular, and in contrast to conjugacy, shifted conjugacy defines no equivalence relation on $B_{\mathbb{N}}$.

Further, Dehornoy proved that the map $f : B_{\mathbb{N}} \to B_{\mathbb{N}}$ defined by $x \mapsto x * e$ is injective for shifted conjugacy [**De99**], while in the case of usual conjugacy we have $f(B_{\mathbb{N}}) = \{e\}$. According to Dehornoy, f might be candidate for an one-way function [**De06**].

Dehornoy points out, that once the definition of shifted conjugacy is used, braids inevitably appear [**De06**]:

Consider a group G, a homomorphism $h : G \to G$, and a fixed element $a \in G$. Then the binary operation

$$x * y = h(x)^{-1} \cdot a \cdot h(y) \cdot x$$

yields an LD-structure on G if and only if the subgroup $H := \langle \{h^n(a) \mid n \in \mathbb{N}\} \rangle \subset G$ is a homomorphic image of $B_{\mathbb{N}}$. For $a = \sigma_1$ and $h = \mathrm{sh}$, which implies $H = B_{\mathbb{N}}$, we get the above defined shifted conjugacy. Of course, we can replace the shift monomorphism sh by any power sh^m for a fixed $m \in \mathbb{N}$.

6. In the case $a = e$ and $h = \mathrm{sh}$, which implies $H = \{e\}$, we get the following left self-distributive operation:

$$x * y = \mathrm{sh} x^{-1} \cdot \mathrm{sh} y \cdot x.$$

We call it simple shifted conjugacy. Simple shifted conjugacy provides not only an LD-structure on $B_{\mathbb{N}}$, but also on the double infinite braid group

$$B_{\mathbb{Z}} =< \{\sigma_i \mid i \in \mathbb{Z}\} \left| \begin{array}{c} \sigma_i\sigma_j = \sigma_j\sigma_i \quad \forall i, j \in \mathbb{Z} : \; |i-j| \geq 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \quad \forall i \in \mathbb{Z} \end{array} \right\rangle.$$

Another LD-structure on $B_{\mathbb{Z}}$ is provided by the operation

$$x \circ y = x \cdot \mathrm{sh}^{-} y \cdot \mathrm{sh}^{-} x^{-1},$$

where sh^{-} denotes the downshift automorphism on $B_{\mathbb{Z}}$ defined by $\sigma_i \mapsto \sigma_{i-1}$ $\forall i \in \mathbb{Z}$. The binary operation $\circ$ is an inverse of the simple shifted conjugacy operation. Indeed, we have

$$x \circ (x * y) = y \quad \text{and} \quad x * (x \circ y) = y \quad \forall x, y \in B_{\mathbb{Z}}.$$

We note that in case of simple shifted conjugacy the function $f : x \mapsto x * e = x\mathrm{sh}x^{-1}$ is (obviously) injective, too.

Examples for RD-systems are easily obtained from this list, becauce if $(S, *)$ is an LD-system, then $(S, \bar{*})$ equipped with $x \bar{*} y = y * x$ is an RD-system.

6.2 Fiat-Shamir-like authentication scheme for LD-systems

Dehornoy proposed the following Fiat-Shamir-like authentication scheme for LD-systems [**De06**].
Let $(S, *)$ be an LD-system. Alice's private key is an element $s \in S$, and her public key is a pair $(x, x') \in S^2$ with $x' = s * x$.
In the authentication phase Alice (the prover) and Bob (the verifier) repeat the following three exchanges k times.

1. Alice selects a random element $r \in S$, and she sends the commitment $(c, c') = (r * x, r*, x')$ to Bob.

2. Bob chooses a random bit $b \in \{0, 1\}$ and transmits it to Alice.

3.0 If $b = 0$, then Alice sends $r_0 = r$, and Bob checks $c \overset{?}{=} r_0 * x$ and $c' \overset{?}{=} r_0 * x'$.

3.1 If $b = 1$, then Alice sends $r_1 = r * s$, and Bob checks $c' \overset{?}{=} r_1 * c$.

The verification for $b = 0$ is obvious, and because of $r_1 * c = (r * s) * (r * x) \overset{LD}{=} r * (s * x) = r * x' = c'$, Bob verifies Alice's secret in the case $b = 1$, too.
Dehornoy proposes $S = B_{\mathbb{N}}$ equipped with shifted conjugacy as platform LD-system for this authentication scheme [**De06**]. In this case this authentication scheme is based on the

ShCSP (Shifted Conjugacy Search Problem):
INPUT: A pair $(x, x') \in B_{\mathbb{N}}^2$ with $x' = s * x$ for some $s \in B_{\mathbb{N}}$.
OBJECTIVE: Find a $\tilde{s} \in B_{\mathbb{N}}$ such that $\tilde{s} * x = x'$.

Note that contrary to the CSP, no solution to the ShCSP in braid groups is known so far. Further it is not known whether the shifted conjugacy decision problem is solvable.
Dehornoy points out that the ShCSP is not a priori immune against general

length attacks [**De06**]. Nevertheless, at the current stage, length attacks do not seem to affect the CSP or even the SCSP (for cryptographically relevant parameters) [**GK$^+$02**, **GK$^+$06**].
Therefore, this Fiat-Shamir-like authentication scheme based on the ShCSP seems to provide more cryptographic security than e.g. scheme II from [**SDG06**], which is based on the CSP.
Further, we consider a slight modification of Dehornoy's authentication scheme. Assume that Alice sends in the case $b = 1$ the response $r' = s * r$ instead of $r * s$, and Bob still checks $c' \overset{?}{=} r' * c$. Then Bob verifies Alice's secret only if $(s * r) * (r * x) = r * (s * x)$ holds. This identity has not been studied so far. It is similar to the central duplication law (CD) $(r * s) * (s * x) = r * (s * x)$ studied in [**De02a**]. It would be interesting to construct a geometry monoid, which exists for every identity (even every family of identities) [**De93**], as in [**De94**, **De02a**] also for this "modified" CD law. Nevertheless, natural examples are still missing.
At a workshop in Bochum in November 2005 Dehornoy proposed a further FS-like authentication scheme for LD-systems [**De05**]. Here Alice's (the prover) public key is $x = s * s$, where s denotes her secret key. Alice and Bob repeat k times the following three-pass protocol.

1. Alice selects a random element $r \in S$, and she sends the commitment $c = r * x$ to Bob.

2. Bob chooses a random bit $b \in \{0, 1\}$ and transmits it to Alice.

3.0 If $b = 0$, then Alice sends $r_0 = r$, and Bob checks $c \overset{?}{=} r_0 * x$.

3.1 If $b = 1$, then Alice sends $r_1 = r * s$, and Bob checks $c \overset{?}{=} r_1 * r_1$.

The verification for $b = 0$ is obvious, and because of $r_1 * r_1 = (r * s) * (r * s) \overset{LD}{=} r * (s * s) = r * x = c$, Bob verifies Alice's secret in the case $b = 1$, too. This scheme comes naturally from Scheme III in [**SDG06**], if we replace conjugacy and the group operation by a general left self-distibutive operation $*$. But accidently, and in contrast to Scheme III in [**SDG06**], this scheme is unsuitable, because a cheater achieves a successful impersonation by repeated transmission of the constant commitment $c = x * x$ and the constant response (for $b = 0, 1$) $r_0 = r_1 = r$.
Nevertheless, this authentication scheme can be easily repaired by setting, e.g., $x = s * (s * s)$, or in general, $x = T_*(s, \ldots, s)$, which denotes a planar rooted binary tree whose leaves are all labelled by s. The subscript $*$ indicates that the grafting of subtrees of T corresponds to the composition $*$. The tree

T is publicly known, and Bob has to check $c \overset{?}{=} T_*(r_1, \ldots, r_1)$ in the case $b = 1$. Now, the verification of Alice' secret succeeds because of

$$T_*(r_1, \ldots, r_1) = T_*(r * s, \ldots, r * s) = r * T_*(s, \ldots, s) = r * x = c,$$

where the second equality in this chain is a straightforward consequence of left self-distributivity.
This authentication scheme is based either on the ShCSP or on the following

Root Finding Problem in $(S, *)$:
INPUT: A planar rooted binary tree T with grafting $*$ and an element $x \in S$ with $x = T_*(s, \ldots, s)$ for some unknown $s \in S$.
OBJECTIVE: Find an element $s' \in S$ such that $T_*(s', \ldots, s') = x$.

While the ShCSP seems to provide much cryptographic security, Dehornoy's authentication schemes are still the only cryptographic primitives based on the ShCSP. In particular, it seems that no key agreement scheme which is based on the ShCSP has been proposed so far. We will close this gap in section 6.4. In the next section we consider a generalization of the AAG scheme. The key agreement for LD-systems turns out to be the most natural special case of this general AAG scheme.

6.3 AAG scheme for magmas

6.3.1 General AAG key agreement protocol

Monoids are proposed as algebraic platform structures for the AAG key agreement protocol in [**AAG99**]. But the monoid structure is only used in the AAG scheme in order to guarantee that the secret key, e.g. Alice's key a, is an uniquely defined product of some given generators $\{s_1, \ldots, s_m\}$, i.e. $a = r_1 \cdot r_2 \cdots r_k$ with $r_i \in \{s_1, \ldots, s_m\}$ for all i. It is, of course, no problem to introduce brackets in this expression. Therefore, there exists a straightforward generalization of the AAG scheme from monoids to magmas[1]. We describe the AAG key establishment protocol in the - for our purposes - most general manner.
Let $(M, \bullet_i)$ and $(N, \circ_i)$ be magmas, for $i = 1, 2$, i.e. there are two operations

[1] A magma (sometimes also called grupoid) $(M, *)$ is a set M equipped with a binary operation $*$ on M, i.e. a function $M \times M \to M$. Note that there are no relations, which have to be satisfied by the elements of M. The notion of a magma was introduced by N. Bourbaki (see, e.g., [**Bo74**]).

on the sets M, N, respectively, and let S be a set. For $i = 1, 2$, we need functions

$$\beta_i : S \times M \to N, \quad \gamma_i : S \times N \to N, \quad p_i : S \to M$$

which satisfy the following three conditions:

(1) $\beta_i(x, \cdot) : M \to N$ is for all $x \in S$ a magma homomorphism[2], i.e.

$$\forall x \in S, y_1, y_2 \in M : \quad \beta_i(x, y_1 \bullet_i y_2) = \beta_i(x, y_1) \circ_i \beta_i(x, y_2).$$

(2) It is, in general, not feasible to determine a secret $x \in S$ from the knowledge of

$$y_1, y_2, \ldots, y_k \in M \quad \text{and} \quad \beta_i(x, y_1), \beta_i(x, y_2), \ldots, \beta_i(x, y_k).$$

(3) For all $a, b \in S$: $\quad \gamma_1(a, \beta_1(b, p_1(a))) = \gamma_2(b, \beta_2(a, p_2(b)))$.

Consider an element y of a magma $(M, \bullet)$ which is an iterated product of other elements in M. Such an element can be described by a planar rooted binary tree T whose k leaves are labelled by these other elements $y_1, \ldots, y_k \in M$. We use the notation $y = T_\bullet(y_1, \ldots, y_k)$. Here the subscript $\bullet$ tells us that the grafting of subtrees of T corresponds to the operation $\bullet$. Now, it is easy to prove by induction that any magma homomorphism $\beta : (M, \bullet) \to (N, \circ)$ satisfies

$$\beta(T_\bullet(y_1, \ldots, y_k)) = T_\circ(\beta(y_1), \ldots, \beta(y_k))$$

for all $y_1, \ldots, y_k \in M$. In particular, the magma morphisms $\beta_1(x, \cdot), \beta_2(x, \cdot)$ $(x \in S)$ fulfill this property.
Alice and Bob publicly assign sets $\{s_1, \ldots, s_m\}, \{t_1, \ldots, t_n\} \subset M$, respectively. The secret key spaces SK_A, SK_B of Alice and Bob are subsets of S, and they depend on these public elements. Indeed, we have

$$SK_A = F_A(s_1, \ldots, s_m) \quad \text{and} \quad SK_B = F_B(t_1, \ldots, t_n).$$

Therefore, it is sufficient that β_1, β_2 fulfill condition (1) only for all $x \in SK_A, SK_B$, respectively, and that condition (3) holds for all $a \in SK_A, b \in SK_B$.
Now, Alice and Bob perform the following protocol steps.

1.A. Alice generates her secret key $a \in SK_A$.

[2] More on magmas and magma homomorphisms can be found, e.g. in [**Se65**, **Ge94**].

1.B. Bob chooses his secret key $b \in SK_B$.

2.A. Alice computes the elements $\beta_2(a, t_1), \ldots, \beta_2(a, t_n) \in N$, and sends them to Bob.

2.B. Analogously Bob computes the elements $\beta_1(b, s_1), \ldots, \beta_1(b, s_m) \in N$, and sends them to Alice.

3.A. Alice, knowing $p_1(a) = T_{\bullet_1}(r_1 \cdots r_k)$ with $r_i \in \{s_1, \ldots, s_m\}$, computes from Bob's public key

$$T_{\circ_1}(\beta_1(b, r_1) \cdots \beta_1(b, r_k)) = \beta_1(b, T_{\bullet_1}(r_1 \cdots r_k)) = \beta_1(b, p_1(a)).$$

3.B. And Bob, knowing $p_2(b) = T'_{\bullet_2}(u_1 \cdots u_{k'})$ with $u_j \in \{t_1, \ldots, t_n\}$, computes from Alice's public key

$$T'_{\circ_2}(\beta_2(a, u_1) \cdots \beta_2(a, u_{k'})) = \beta_2(a, T'_{\bullet_2}(u_1 \cdots u_{k'})) = \beta_2(a, p_2(b)).$$

4.A. Alice computes $K := \gamma_1(a, \beta_1(b, p_1(a)))$.

4.B. Bob also computes the shared key $\gamma_2(b, \beta_2(a, p_2(b))) \overset{(3)}{=} K$.

First we consider the most natural special case of this scheme. Let be $M = N = S$. This implies that the functions β_i, γ_i, for $i = 1, 2$, induce further binary operations on M. In particular, we introduce the notation $x *_i y = \beta_i(x, y)$. Now, the homomorphy condition (1) reads as

$$x *_i (y_1 \bullet_i y_2) = (x *_i y_1) \circ_i (x *_i y_2) \quad \forall x, y_1, y_2 \in M \ (i = 1, 2).$$

If additionally $*_i = \bullet_i = \circ_i$ holds for $i = 1, 2$, then M is an LD-system with two (left) self-distributive operations $*_1, *_2$. A key agreement using two LD-structures on the infinite braid group is described in section 6.4.
Another specification of our general magma-based scheme is discussed in the next subsection.

6.3.2 AAG-like scheme based on a simultaneous decomposition problem

We consider the following specifications of the AAG scheme for magmas:
Let $G = M = N$ be a group, and set $S = G^2$. The group multiplication symbol in G will usually be omitted. The operations $\bullet_i, \circ_i$ $(i = 1, 2)$ on G are defined by

$$x \bullet_1 y = x \bullet_2 y = x \circ_1 y = x \circ_2 y \equiv x \bullet y := xy^{-1}x,$$

and the functions $\beta_1, \beta_2 : G^2 \times G \to G$ are defined by

$$\beta_1((x_1,x_2),y) = \beta_2((x_1,x_2),y) \equiv \beta((x_1,x_2),y) := x_1yx_2.$$

$\beta(x,\cdot)$ fulfills the homomorphy condition (1), for all $x = (x_1,x_2) \in G^2$, because

$$\begin{aligned} \beta((x_1,x_2),y_1) \bullet \beta((x_1,x_2),y_2) &= (x_1y_1x_2) \bullet (x_1y_2x_2) = \\ (x_1y_1x_2)x_2^{-1}y_2^{-1}x_1^{-1}(x_1y_1x_2) &= x_1(y_1y_2^{-1}y_1)x_2 = \beta((x_1,x_2),y_1 \bullet y_2). \end{aligned}$$

Alice and Bob publicly assign sets $\{s_1,\dots,s_m\}, \{t_1,\dots,t_n\} \subset G$, respectively. The secret key spaces of Alice and Bob are $SK_A = G \times S_A$ and $SK_B = S_B \times G$, where $S_A = \langle s_1,\dots,s_m\rangle_\bullet$ and $S_B = \langle t_1,\dots,t_n\rangle_\bullet$ denote submagmas of $(G,\bullet)$ generated by the publicly assigned elements.
The projections $p_1, p_2 : G^2 \to G$ and the functions $\gamma_1, \gamma_2 : G^2 \times G \to G$ are defined by

$$p_1(x,y) = y, \; p_2(x,y) = x \quad \text{and} \quad \gamma_1((x_1,x_2),y) = x_1y, \; \gamma_2((x_1,x_2),y) = yx_2.$$

These definitions satisfy condition (3), because

$$\begin{aligned} & \gamma_1(a,\beta(b,p_1(a))) = \gamma_1(a,\beta(b,a_r)) = \gamma_1(a,b_la_rb_r) = a_l(b_la_rb_r) \\ = \; & (a_lb_la_r)b_r = \gamma_2(b,a_lb_la_r) = \gamma_2(b,\beta(a,b_l)) = \gamma_2(b,\beta(a,p_2(b))) \end{aligned}$$

for all $a = (a_l,a_r), b = (b_l,b_r) \in G^2$.
Now, consider the right part of Alice's key $a_r = T_\bullet(r_1,\dots,r_k) \in S_A$ with $r_i \in \{s_1,\dots,s_m\}$. If we view a_r as a word in the s_i's, then we observe that a_r is self-reverse and the exponent signs of a_r alternate, beginning and ending with a positive sign. For example, we have

$$(r_1 \bullet r_2) \bullet (r_3 \bullet (r_4 \bullet r_5)) = r_1r_2^{-1}r_1r_3^{-1}r_4r_5^{-1}r_4r_3^{-1}r_1r_2^{-1}r_1.$$

While in this scheme alternating exponent signs are essential to gurantee that condition (1) holds, the self-reverse property turns out to be superflous. Therefore, we give up this restricted key choice and define modified secret key spaces by $SK_A = G \times SK_A^{(r)}$ and $SK_B = SK_B^{(l)} \times G$ with

$$\begin{aligned} SK_A^{(r)} &= \{r_1r_2^{-1}r_3r_4^{-1}\cdots r_{2l}^{-1}r_{2l+1} \mid r_i \in \{s_1,\dots,s_m\} \, \forall 1 \le i \le l, l \in \mathbb{N}\}, \\ SK_B^{(l)} &= \{u_1u_2^{-1}u_3u_4^{-1}\cdots u_{2l'}^{-1}u_{2l'+1} \mid u_j \in \{t_1,\dots,t_n\} \, \forall 1 \le j \le l', l' \in \mathbb{N}\}. \end{aligned}$$

Alice and Bob have to perform the following protocol steps.

1.A. Alice generates her secret key $(a_l,a_r) \in G \times SK_A^{(r)}$.

1.B. Bob chooses his secret key $(b_l, b_r) \in SK_B^{(l)} \times G$.

2.A. Alice computes the elements $a_l t_1 a_r, \ldots, a_l t_n a_r$, and sends them to Bob.

2.B. Analogously Bob computes the elements $b_l s_1 b_r, \ldots, b_l s_m b_r$, and sends them to Alice.

3.A. Alice, knowing $a_r = r_1 r_2^{-1} r_3 r_4^{-1} \cdots r_{2l}^{-1} r_{2l+1}$ with $r_i \in \{s_1, \ldots, s_m\}$, computes from Bob's public key

$$\begin{aligned} & (b_l r_1 b_r)(b_l r_2 b_r)^{-1}(b_l r_3 b_r) \cdots (b_l r_{2l} b_r)^{-1}(b_l r_{2l+1} b_r) \\ = \ & b_l(r_1 r_2^{-1} r_3 \cdots r_{2l}^{-1} r_{2l+1}) b_r = b_l a_r b_r. \end{aligned}$$

3.B. Bob, knowing $b_l = u_1 u_2^{-1} u_3 u_4^{-1} \cdots u_{2l'}^{-1} u_{2l'+1}$ with $u_j \in \{t_1, \ldots, t_n\}$, computes from Alice's public key

$$\begin{aligned} & (a_l u_1 a_r)(a_l u_2 a_r)^{-1}(a_l u_3 a_r) \cdots (a_l u_{2l'} a_r)^{-1}(a_l u_{2l'+1} a_r) \\ = \ & a_l(u_1 u_2^{-1} u_3 \cdots u_{2l'}^{-1} u_{2l'+1}) a_r = a_l b_l a_r. \end{aligned}$$

4.A. Alice computes $K := a_l(b_l a_r b_r)$.

4.B. Bob also computes the shared key $(a_l b_l a_r) b_r = K$.

In order to break this scheme an attacker obviously has to solve the following

Base Problem:
INPUT: Element pairs $(s_1, s_1'), \ldots, (s_m, s_m') \in G^2$ and $(t_1, t_1'), \ldots, (t_n, t_n') \in G^2$ with $s_i' = b_l s_i b_r \ \forall 1 \leq i \leq m$ and $t_j' = a_l t_j a_r \ \forall 1 \leq j \leq n$ for some (unknown) $a_l, b_r \in G$, $b_l \in SK_B^{(l)}$, $a_r \in SK_A^{(r)}$.
OBJECTIVE: Find $K = a_l b_l a_r b_r$.

A successful attack on Alice's secret key requires the solution of the following

n-**SDP** (n-Simultaneous Decomposition Problem):
INPUT: Element pairs $(t_1, t_1'), \ldots, (t_n, t_n') \in G^2$ with $t_j' = a_l t_j a_r \ \forall 1 \leq j \leq n$ for some (unknown) $a_l \in G$, $a_r \in SK_A^{(r)}$.
OBJECTIVE: Find elements $a_l' \in G$, $a_r' \in SK_A^{(r)}$ with $a_l' t_j a_r' = t_j'$ for all $j = 1, \ldots, n$.

A solution (a_l', a_r') to this n-SDP satisfies the property $a_l' y a_r' = a_l y a_r$ for all $y \in SK_B^{(l)}$.
Analogeously, a successful attack on Bob's secret key requires the solution of the following

m-**SDP** (m-Simultaneous Decomposition Problem):

INPUT: Element pairs $(s_1, s'_1), \ldots, (s_m, s'_m) \in G^2$ with $s'_i = b_l s_i b_r \; \forall 1 \leq i \leq m$ for some (unknown) $b_l \in SK_B^{(l)}$, $b_r \in G$.

OBJECTIVE: Find elements $b'_l \in SK_B^{(l)}$, $b'_r \in G$ with $b'_l s_i b'_r = s'_i$ for all $i = 1, \ldots, m$.

A solution (b'_l, b'_r) to this m-SDP satisfies the property $b'_l x b'_r = b_l x b_r$ for all $x \in SK_A^{(r)}$.

Therefore, a solution to both problems provides the attacker with the shared secret, because

$$(a'_l b'_l a'_r) b'_r = (a_l b'_l a_r) b'_r = a_l (b'_l a_r b'_r) = a_l (b_l a_r b_r) = K.$$

Here the first and the last equality hold, because $b'_l \in SK_B^{(l)}$ and $a_r \in SK_A^{(r)}$, respectively. Alternatively, we can use equality chain

$$a'_l (b'_l a'_r b'_r) = a'_l (b_l a'_r b_r) = (a'_l b_l a'_r) b_r = (a_l b_l a_r) b_r = K,$$

where here the first and the last equality hold, because $a'_r \in SK_A^{(r)}$ and $b_l \in SK_B^{(l)}$, respectively. Further, the first equality chain shows us, that it is sufficient to find a solution $(a'_l, a'_r) \in G^2$ to the n-SDP and a solution $(b'_l, b'_r) \in SK_B^{(l)} \times G$ to the m-SDP. Analogously, the second equality chain shows us, that it is sufficient to find a solution $(a'_l, a'_r) \in G \times SK_A^{(r)}$ to the n-SDP and a solution $(b'_l, b'_r) \in G^2$ to the m-SDP.

Nevertheless, such observations seems to have no practical relevance. A solution (a'_l, a'_r) to Alice's n-SDP satisfies (for all $1 \leq j \leq n$) $a'_l t_j a'_r = a_l t_j a_r$ which is equivalent to $t_j^{-1}(a_l^{-1} a'_l) t_j = a_r (a'_r)^{-1}$. For "generic" instances, it seems to be completely unprobable that nontrivial solutions (a'_l, a'_r) with $a'_l \neq a_l$ and[3] $a'_r \neq a_r$ exist.

But it is very important to note that the knowledge of one secret key, e.g. Alice's key $(a_l, a_r) \in G \times SK_A^{(r)}$, is not sufficient for an attacker to obtain the shared secret K, because he needs not only a_r expressed in the generators of the group G, but rather an expression of the form

$$a_r = r_1 r_2^{-1} r_3 r_4^{-1} \cdots r_{2l}^{-1} r_{2l+1} \quad \text{with} \quad r_i \in \{s_1, \ldots, s_m\}.$$

We close with the trivial remark that Alice can choose the left part of her secret a_l from any arbitrary secret subgroup H_l of G. Analogously, Bob can select b_r from any arbitrary secret $H_r \subset G$.

[3] Note that $a'_l = a_l \Leftrightarrow a'_r = a_r$.

6.4 Key agreement based on shifted conjugacy

Recall from section 6.1 the shifted conjugacy operation $*$ and the "reverse" shifted conjugacy operation $\bar{*}$ in $B_{\mathbb{N}}$ defined by

$$x * y = \mathrm{sh}x^{-1} \cdot \sigma_1 \cdot \mathrm{sh}y \cdot x \quad \text{and} \quad x \bar{*} y = x\mathrm{sh}y \cdot \sigma_1 \mathrm{sh}x^{-1}.$$

Both operations satisfy the left self-distributive law.
We propose a key establishment protocol using these LD-structures in $B_{\mathbb{N}}$, where Alice and Bob have to perform the following protocol steps.

0.A. Alice publicly assigns elements $s_1, \ldots, s_m \in B_{\mathbb{N}}$.

0.B. Bob publicly assigns elements $t_1, \ldots, t_n \in B_{\mathbb{N}}$.

1.A. Alice generates her secret key $a \in S_A$, where $S_A = \langle s_1, \ldots, s_m \rangle_*$ denotes the sub-LD-system of $(B_{\mathbb{N}}, *)$ generated by $\{s_1, \ldots, s_m\}$. Therefore she chooses a planar rooted binary tree T with k leaves and elements $r_1, \ldots, r_k$ with $r_i \in \{s_1, \ldots, s_m\}$ such that $a = T_*(r_1, \ldots, r_k)$.

1.B. Bob chooses his secret key $b \in S_B$, where $S_B = \langle t_1, \ldots, t_n \rangle_{\bar{*}}$ denotes the sub-LD-system of $(B_{\mathbb{N}}, \bar{*})$ generated by $\{t_1, \ldots, t_n\}$. Therefore he chooses a planar rooted binary tree T' with k' leaves and elements $u_1, \ldots, u_{k'}$ with $u_j \in \{t_1, \ldots, t_n\}$ such that $b = T'_{\bar{*}}(u_1, \ldots, u_{k'})$.

2.A. Alice computes the elements $a^{-1} \bar{*} t_1, \ldots, a^{-1} \bar{*} t_n$, and sends them to Bob.

2.B. Analogously Bob computes the elements $b^{-1} * s_1, \ldots, b^{-1} * s_m$, and sends them to Alice.

3.A. Alice, knowing $a = T_*(r_1, \ldots, r_k)$ for some planar rooted binary tree T and $r_i \in \{s_1, \ldots, s_m\}$, computes from Bob's public key

$$T_*(b^{-1} * r_1, \ldots, b^{-1} * r_k) = b^{-1} * T_*(r_1, \ldots, r_k) = b^{-1} * a.$$

3.B. Bob, knowing $b = T_{\bar{*}}(u_1, \ldots, u_{k'})$ for some planar rooted binary tree T' and $u_j \in \{t_1, \ldots, t_n\}$, computes from Alice's public key

$$T_{\bar{*}}(a^{-1} \bar{*} u_1, \ldots, a^{-1} \bar{*} u_{k'}) = a^{-1} \bar{*} T_{\bar{*}}(u_1, \ldots, u_{k'}) = a^{-1} \bar{*} b.$$

4.A. Alice computes $K := a^{-1}(b^{-1} * a) = a^{-1}(\mathrm{sh}b \cdot \sigma_1 \mathrm{sh}a \cdot b^{-1})$.

4.B. Bob also computes the shared key[4]

$$(a^{-1}\bar{*}b)b^{-1} = (a^{-1}\mathrm{sh}b \cdot \sigma_1\mathrm{sh}a)b^{-1} = K.$$

This scheme can be obtained from the AAG key agreement protocol for magmas (section 6.3.1) specified by $M = N = S = B_{\mathbb{N}}$, $\bullet_1 = \circ_1 = *$, $\bullet_2 = \circ_2 = \bar{*}$, $p_1 = p_2 = \mathrm{id}$,

$$\beta_1(x,y) = x^{-1} * y,\ \beta_2(x,y) = x^{-1}\bar{*}y,\ \gamma_1(x,y) = x^{-1}y,\ \gamma_2(x,y) = yx^{-1},$$

and $SK_A = \langle s_1, \ldots, s_m\rangle_*$, $SK_B = \langle t_1, \ldots, t_n\rangle_{\bar{*}}$.

In order to break this scheme an attacker obviously has to solve the following

Base Problem:
INPUT: Pairs $(s_1, s'_1), \ldots, (s_m, s'_m) \in B_{\mathbb{N}}^2$ and $(t_1, t'_1), \ldots, (t_n, t'_n) \in B_{\mathbb{N}}^2$ with $s'_i = b^{-1} * s_i = \mathrm{sh}b \cdot \sigma_1\mathrm{sh}s_i \cdot b^{-1}$ $\forall 1 \leq i \leq m$ and $t'_j = a^{-1}\bar{*}t_j = a^{-1}\mathrm{sh}t_j \cdot \sigma_1\mathrm{sh}a$ $\forall 1 \leq j \leq n$ for some (unknown) $a \in S_A = \langle s_1, \ldots, s_m\rangle_*$, $S_B = \langle t_1, \ldots, t_n\rangle_{\bar{*}}$.
OBJECTIVE: Find $K = a^{-1}(b^{-1} * a) = (a^{-1}\bar{*}b)b^{-1} = a^{-1}\mathrm{sh}b \cdot \sigma_1\mathrm{sh}a \cdot b^{-1}$.

But a successful attack on Bob's secret key requires the solution of the following

m-**SGShCSP** (m-Simultaneous Generalized Shifted Conjugacy Search Problem):

INPUT: Pairs $(s_1, s'_1), \ldots, (s_m, s'_m) \in B_{\mathbb{N}}^2$ with $s'_i = b^{-1} * s_i = \mathrm{sh}b \cdot \sigma_1\mathrm{sh}s_i \cdot b^{-1}$ $\forall 1 \leq i \leq m$ for some (unknown) $b \in S_B$.
OBJECTIVE: Find an element $b' \in S_B$ with $b'^{-1} * s_i = b^{-1} * s_i$ for all $i = 1, \ldots, m$.

Analogously, Alice's secret can be attacked by solving a n-simultaneous (reverse) shifted conjugacy search problem.

n-**SGShCSP** (n-Simultaneous Generalized Shifted Conjugacy Search Problem):

INPUT: Pairs $(t_1, t'_1), \ldots, (t_n, t'_n) \in B_{\mathbb{N}}^2$ with $t'_j = a^{-1}\bar{*}t_j = a\mathrm{sh}t_j \cdot \sigma_1\mathrm{sh}a^{-1}$ $\forall 1 \leq i \leq n$ for some (unknown) $a \in S_A$.
OBJECTIVE: Find an element $a' \in S_A$ with $a'^{-1}\bar{*}t_j = a^{-1}\bar{*}t_j$ for all $j = 1, \ldots, n$.

[4] If we define the shifted commutator as $[a,b]^{\mathrm{sh}} = a^{-1}\mathrm{sh}b^{-1} \cdot \sigma_1\mathrm{sh}a)b$, then the shared key is $K = [a, b^{-1}]^{\mathrm{sh}}$.

Since a solution $b' \in S_B$ to the m-SGShCSP satisfies the property $b'^{-1} * x = b^{-1} * x$ for all $x \in S_A$, a solution to both problems (m-SGShCSP and m-SGShCSP) provides the attacker with the shared secret, because

$$a'^{-1}(b'^{-1} * a') = a'^{-1}(b^{-1} * a') = (a'^{-1} \bar{*} b)b^{-1} = (a^{-1} \bar{*} b)b^{-1} = K.$$

Here the last equality holds, because $b \in S_B$. We observe that it is sufficient to find a solution $a' \in B_{\mathbb{N}}$ to the n-SGShCSP and a solution $b' \in S_B$ to the m-SGShCSP.
Analogously, a solution $a' \in S_A$ to the n-SGShCSP satisfies the property $a'^{-1} \bar{*} y = a^{-1} \bar{*} y$ for all $y \in SK_B$. Therefore, we can also use the equality chain

$$(a'^{-1} \bar{*} b')b'^{-1} = (a^{-1} \bar{*} b')b'^{-1} = a^{-1}(b'^{-1} * a) = a^{-1}(b^{-1} * a) = K.$$

Here the last equality holds, because $a \in S_A$. We observe that it is sufficient to find a solution $a' \in S_A$ to the n-SGShCSP and a solution $b' \in B_{\mathbb{N}}$ to the m-SGShCSP.
Nevertheless, as in section 6.3.2, such observations seems to have no practical relevance. A solution a' to Alice's n-SGShCSP satisfies (for all $1 \leq j \leq n$) $a'^{-1} \bar{*} t_j = a^{-1} \bar{*} t_j$ which is equivalent to

$$a' \mathrm{sh} t_j \cdot \sigma_1 \mathrm{sh} a'^{-1} = a \mathrm{sh} t_j \cdot \sigma_1 \mathrm{sh} a^{-1} \quad \forall 1 \leq j \leq n.$$

For "generic" instances, it seems to be unprobable to us that there exists a nontrivial solution a' with $a' \neq a$.
But it is very important to note, that the knowledge of one secret key, e.g. Alice's key $a \in S_A$, is not sufficient for an attacker to obtain the shared secret K, because he needs not only a expressed in the generators of $B_{\mathbb{N}}$, but rather an expression of the form

$$a = T_*(r_1, \ldots, r_k) \quad \text{with} \quad r_i \in \{s_1, \ldots, s_m\}$$

where T is a planar rooted binary tree with grafting $*$.

Since the base problem of our key agreement scheme is a multi-simultaneous search problem, where several shifted conjugated pairs are given, length attacks may apply very well against this problem. Nevertheless, at the current stage, pure length attacks do not seem to affect the SCSP (a related problem) for cryptographically relevant parameters [**GK⁺02**, **GK⁺06**].

Bibliography

[**AA93**] Iris Anshel and Michael Anshel, *From the Post-Markov theorem through decision problems to public-key cryptography*, Amer. Math. Monthly **100** (1993), 835-845.

[**AA$^+$01**] Iris Anshel, Michael Anshel, Benji Fisher and Dorian Goldfeld, *New Key Agreement Protocols in Braid Group Cryptography*, Topics in Cryptology - CT-RSA 2001, LNCS **2020**, Springer-Verlag (2001), 13-27.

[**AAG99**] Iris Anshel, Michael Anshel and Dorian Goldfeld, *An algebraic method for public-key cryptography*, Mathematical Research Letters **6** (1999), 1-5.

[**AAG03**] Iris Anshel, Michael Anshel and Dorian Goldfeld: *Non-abelian key agreement protocols*, Discrete Applied Mathematics **130** (2003), 3-12.

[**AAG06**] Iris Anshel, Michael Anshel and Dorian Goldfeld: *A linear time matrix key agreement protocol over small finite fields*, Applicable Algebra in Engineering, Communication and Computing **17** (2006), 195-203.

[**AK06**] Peter Ackermann and Martin Kreuzer, *Gröbner basis cryptosystems*, Applicable Algebra in Engineering, Communication and Computing **17** (2006), 173-194.

[**AM99**] Peter Abramenko and Thomas W. Müller, *Are braid groups linear groups? Remarks on a paper of S. Bachmuth*, Preprint-Server of the SFB 343 "Diskrete Strukturen in der Mathematik", Preprint 99-100 (1999), `http://www.mathematik.uni-bielefeld.de/sfb343/preprints/index99.html` - Also available from: `http://citeseer.ist.psu.edu/268408.html`

[**Ar26**] Emil Artin, *Theorie der Zöpfe*, Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität **4** (1926), 47-72.

[**Ar47**] Emil Artin, *Theory of braids*, Annals of Math. (2) **48** (1947), 101-126.

[**Ba96**] Seymour Bachmuth, *Braid groups are linear groups*, Adv. Math. **121** (1996), 50-61.

[**Ba02a**] Patrick D. Bangert, *Algorithmic Problems in the Braid Groups*, Dissertation: Department of Mathematics, University College London (2002).

[**Ba02b**] Patrick D. Bangert, *Algorithmic Problems in the Braid Groups*, Journal Phys. A **35** (2002), 43-59.

[**Ba04**] Patrick D. Bangert, *Raid Braid: Fast Conjugacy Disassembly in Braid and Other Groups*, to appear in: Proceedings of Applications of Computer Algebra (ACA-2004).

[**Ba07**] Patrick D. Bangert, *The Conjugacy Problem in B_n*, In: I. Anshel, M. Anshel and D. Goldfeld (Eds.), *Contributions to Contemporary Cryptography*, Singapore, World Scientific Pub. Co (2007).

[**BB06**] Joan S. Birman and Tara E. Brendle, *Braids: A Survey*, In: W. Menasco and M. Thistlethwaite (Eds.), *Handbook of Knot Theory*, Elsevier (2006). Eprint archive: `arXiv:math.GT/0409205`

[**BC$^+$06**] G. Baumslag, T. Camps, B. Fine, G. Rosenberger and X. Xu, *Designing Key Transport Protocols Using Combinatorial Group Theory.* In: L. Gerritzen, D. Goldfeld, M. Kreuzer, G. Rosenberger and V. Shpilrain (Eds.), *Algebraic Methods in Cryptography*, Contemporary Mathematics **418**, AMS (2006), 35-43.

[**BD99**] V. N. Bezverkhnii and I. V. Dobrynina, *On the Unsolvability of the Conjugacy Problem for Subgroups of the Group R_5 of Pure Braids*, Mathematical Notes **65**, no. 1 (1999), 13-19.

[**Be94**] M. A. Berger, *Minimum crossing numbers for 3-braids*, Journal of Physics A **27** (1994), 6205-6213.

[**Be03**] David Bessis, *The dual braid monoid*, Ann. Sci. Ecole Norm. Sup. **36**, no. 5 (2003), 647-683. Eprint archive: `arXiv:math.GR/0101158`.

[**BGG06a**] Joan Birman, Volker Gebhardt and Juan Gonzales-Meneses, *Conjugacy Search in Garside groups I: Cyclings, Powers and Rigidity.* Eprint archive: `arXiv:math.GT/0605230`

[**BGG06b**] Joan Birman, Volker Gebhardt and Juan Gonzales-Meneses, *Conjugacy Search in Garside groups II: Structure of the Ultra summit Set.* Eprint archive: `arXiv:math.GT/0606652`

[BGG06c] Joan Birman, Volker Gebhardt and Juan Gonzales-Meneses, *Conjugacy Search in Garside groups III: Periodic Braids.* Eprint archive: `arXiv:math.GT/0609616`

[Bi74] Joan S. Birman, *Braids, links and mapping class groups*, Annals of Mathematics Studies **82**, Princeton University Press (1974).

[Bi98] Joan S. Birman, *Review of* [**Ba96**], Math. Reviews 98h :20061.

[Bi99] Stephen J. Bigelow, *The Burau representation is not faithful for* $n =$ 5, Geom. Topol. **3** (1999), 397-404.

[Bi00] Stephen J. Bigelow, *Homological Representations of Braid Groups*, Dissertation, University of California, Berkeley (2000).

[Bi01] Stephen J. Bigelow, *Braid groups are linear*, J. Amer. Math. Soc. **14**, no. 2 (2001), 471-486.

[Bi02] Stephen J. Bigelow, *Does the Jones polynomial detect the unknot?*, Journal of Knot Theory and Its Ramifications **11**, no. 4 (2002), 493-505.

[BKL98] Joan S. Birman, Ki Hyoung Ko, Sang Jin Lee, *New approaches to the word and conjugacy problem in the braid groups*, Advances in Math. **139** (1998), 322-353. Eprint archive: `arXiv:math.GT/9712211`

[BKL01] Joan S. Birman, Ki Hyoung Ko and Sang Jin Lee, *The infimum, supremum and geodesic length of a braid conjugacy class*, Advances in Mathematics **164** (2001), 41-56. Eprint archive: `arXiv:math.GT/0003125`

[Bl53] Leonard M. Blumenthal, *Theory and Applications of Distance Geometry*, OxfordUniversity Press (1953).

[BLM92] Joan S. Birman, Darren D. Long and John A. Moody, *Finite-Dimensional Representations of Artin's Braid Group*, in: Abikoff, Birman and Kuiken (eds.): *The mathematical legacy of Wilhelm Magnus: Groups, Geometry and special functions*, Contemporary Mathematics **169**, AMS (1992).

[BM03] Colin Boyd and Anish Mathuria, *Protocols for Authentication and Key Establishment*, Springer-Verlag (2003).

[BMR98] Michel Broué, Gunther Malle and Raphaël Rouquier, *Complex reflection groups, braid groups, Hecke algebras*, J. Reine Angew. Math. **500** (1998), 127-190.

[**BMS06**] Jean-Camille Birget, Spyros S. Magliveras and Michal Sramka, *On public-key cryptosystems based on combinatorial group theory*, Tatra Mountains Mathematical Publications **33** (2006), 137-148.
Earlier version: `http://eprint.iacr.org/2005/070`

[**Bo54**] William W. Boone, *Certain simple unsolvable problems of group theory*, Indig. Math. **16** (1954), 231-237, 492-497.

[**Bo74**] Nicholas Bourbaki, *Elements of Mathematics: Algebra I*, Hermann (1974).

[**Br94**] Thomas Brady, *Automatic structures on $Aut(F_2)$*, Arch. Math. **63** (1994), 97-102.

[**BS72**] E. Brieskorn und K. Saito, *Artin-Gruppen und Coxeter-Gruppen*, Invent. Math. **17** (1972), 245-271.

[**Bu36**] Werner Burau, *Über Zopfgruppen und gleichsinnig verdrillte Verkettungen*, Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität **11** (1936), 179-186.

[**BW89**] Joan S. Birman and Hans G. Wenzl *Braids, link polynomials and a new algebra*, Trans. Amer. Math. Soc. **313** (1989), 249-273.

[**BZ03**] Gerhard Burde and Heiner Zieschang, *Knots*, 2nd Edition, de-Gruyter (2003).

[**CA90**] David Chaum and Hans van Antwerpen, *Undeniable Signatures*, Advances in Cryptology, Proceedings of CRYPTO 89, LNCS **435** (1990), 212-217.

[**Ch48**] Wei-Liang Chow, *On the algebraic braid group*, Annals of Math. **49** (1948), 654-658.

[**Ch86**] David Chaum, *Showing credentials without identification*, Advances in Cryptology: Proceedings of EUROCRYPT 85, LNCS **219** (1986), 241-244.

[**CH91**] David Chaum and Eugene van Heijst, *Group signatures*, Advances in Cryptology: Proceedings of Eurocrypt 91, LNCS **547** (1991), 241-246.

[**Ch92**] Ruth Charney, *Artin groups of finite type are biautomatic*, Math. Ann. **292** (1992), 671-683.

[Ch95] Ruth Charney, *Geodesic automation and growth functions for Artin groups of finite type*, Math Ann. **301** (1995), 307-324.

[CDW07] Zhenfu Cao, Xiaolei Dong and Licheng Wang, *New Public Key Cryptosystems Using Polynomials over Non-commutative Rings*, Cryptology eprint archive: `http://eprint.iacr.org/2007/009`

[CJ03a] Jung Hee Cheon and Byungheup Jun, *Diffie-Hellman Conjugacy Problem on Braids*, Preprint, electronically available from: `http://citeseer.ist.psu.edu/557008.html`

[CJ03b] Jung Hee Cheon and Byungheup Jun, *A Polynomial Time Algorithm for the Braid Diffie-Hellman Conjugacy Problem*, Advances in Cryptology - CRYPTO 2003, LNCS **2729**, Springer (2003).

[CK$^+$01] Jae Choon Cha, Ki Hyoung Ko, Sang Jin Lee, Jae Woo Han and Jung Hee Cheon, *An efficient implementation of braid groups*, Advances in Cryptology - ASIA-CRYPT 2001, LNCS **2248**, Springer (2001).

[CL92] Florin Constantinescu and Mirko Lüdde, *Braid Modules*, Journal of Physics A: Math. Gen. **25** (1992), L1273-L1280.

[CL95] Florin Constantinescu and Mirko Lüdde, *The Alexander- and Jones-Invariants and the Burau Module*, Preprints Archive of the Sfb 288: Differential Geometry and Quantum Physics, preprint no. 181 (1995), `http://www-sfb288.math.tu-berlin.de/Publications/preprint-list/151/200` - Also available from: `http://citeseer.ist.psu.edu/222988.html`

[CM04] Ruth Charney and John Meier, *The language of geodesics of Garside groups*, Math. Zeitschrift **248** (2004), 495-509.

[Co89] Daniel E. Cohen, *Combinatorial Group Theory: A Topological Approach*, Cambridge University Press, New York (1989).

[Co94] Donald J. Collins, *Relations among the squares of the generators of the braid group*, Invent. Math. **117** (1994), 525-529.

[Co03] Computational Algebra Group, *MAGMA 2.10*, University of Sydney (2003), `magma.maths.usyd.edu.au/magma/`

[CT93] Florin Constantinescu and Francesco Toppan, *On the Linearized Artin Braid Representation*, Intern. Journ. of Knots and Its Ramifications **2** (1993), 399-412.

[CW02] Arjeh M. Cohen and David B. Wales, *Linearity of Artin groups of finite type*, Israel J. Math. **131** (2002), 101-123.

[DD$^+$02] P. Dehornoy, I. Dynnikov, D. Rolfsen and B. Wiest, *Why are braids orderable?*, Société Mathématique de France (2002).

[De11] Max Dehn, *Über unendliche diskontinuierliche Gruppen*, Math. Annalen **71** (1911), 116-144.

[De72] Pierre Deligne, *Les immeubles des groupes de tresses géenéralisés*, Invent. Math. **17** (1972), 273-302.

[De93] Patrick Dehornoy, *Structural monoids associated to equational varieties*, Proc. Amer. Math. Soc. **117** (2) (1993), 293-304.

[De94] Patrick Dehornoy, *Braid groups and left distributive opreations*, Trans. Amer. Math. Soc **345-1** (1994), 115-151.

[De97] Patrick Dehornoy, *A fast method for comparing braids*, Adv. in Math. **125** (1997), 200-235.

[De98] Patrick Dehornoy, *Gaussian groups are torsion free*, Journal of Algebra **210** (1998), 291-297.

[De99] Patrick Dehornoy, *Strange questions about braids*, J. Knot Th. and its Ramifications **8** (5) (1999), 589-620.

[De00] Patrick Dehornoy, *Braids and Self-Distributivity*, Progress in Math. **192** Birkhäuser (2000).

[De02a] Patrick Dehornoy, *Study of an identity*, Algebra Universalis **48** (200), 223-248.

[De02b] Patrick Dehornoy, *Groupes de Garside*, Ann. Sc. Ec. Norm. Sup. **35** (2002), 267-306.

[De04a] Patrick Dehornoy, *The group of fractions of a torsion free lcm monoid is torsion free*, Journal of Algebra **281**, no. 1 (2004), 303-305.

[De04b] Patrick Dehornoy, *Braid-based cryptography*, Contemporary Mathematics **360** (2004), 5-33.

[De05] Patrick Dehornoy, *Braid-based cryptography.* Talk at the International Workshop on Algebraic Methods in Cryptography, Nov. 17-18, 2005. Talk slides currently avialable from:
`http://www.math.unicaen.fr/~dehornoy/talks.html`

[De06] Patrick Dehornoy, *Using shifted conjugacy in braid-based cryptography.* In: L. Gerritzen, D. Goldfeld, M. Kreuzer, G. Rosenberger and V. Shpilrain (Eds.), *Algebraic Methods in Cryptography*, Contemporary Mathematics **418**, AMS (2006), 65-73.

[DH76] Whitfield Diffie und Martin E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory **22** (1976), 644-654.

[Di03] Francois Digne, *On the linearity of Artin braid groups*, Journal of Algebra **268**, no.1 (2003), 39-57.

[DL97] Michel Marie Deza and Monique Laurent, *Geometry of Cuts and Metrics*, Algorithms and Combinatorics **15**, Springer (1997).

[DP99] Patrick Dehornoy and Luis Paris, *Gaussian groups and Garside groups, two generalizations of Artin groups*, Proc. London Math. Soc. **79-3** (1999), 569-604.

[Dy02] Ivan Dynnikov, *On a Yang-Baxter mapping and the Dehornoy ordering*, Uspekhi Mat. Nauk **57**, no. 3 (2002), 151-152; English translation in: Russian Math. Surveys **57**, no. 3 (2002).

[EC$^+$92] David B. A. Epstein, James W. Cannon, Derek F. Holt, Silvio V. F. Levy, Michael S. Paterson and William P. Thurston, *Word processing in groups*, Jones and Bartlett (1992).

[EK04] Bettina Eick and Delaram Kahrobaei, *Polycyclic groups: a new platform for cryptography*, Eprint archive: `arXiv:math.GR/0411077` (2004).

[El85] Taher ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory **31** (1985), 469-472.

[EM94] Elsayed A. Elrifai and Hugh R. Morton, *Algorithms for positive braids*, Quart. J. Math. **45** (1994), 479-497.

[FFS88] Uriel Feige, Amos Fiat and Adi Shamir, *Zero-Knowledge Proofs of Identity*, Journal of Cryptology **1** (1988), 77-94.

[FG02] Nuno Franco and Juan Gonzalez-Meneses, *Computation of Normalizers in Braid groups and Garside Groups*,
Eprint archive: `arXiv:math.GT/0201243`

[**FG03a**] Nuno Franco and Juan Gonzalez-Meneses, *Conjugacy problem for braid groups and Garside groups*, Journal of Algebra **266** (1) (2003), 112-132. Eprint archive: `arXiv:math.GT/0112310`

[**FG03b**] Nuno Franco and Juan Gonzalez-Meneses, *Computation of Centralizers in Braid groups and Garside Groups*, Rev. Mat. Iberoamericana **19** (2) (2003), 367-384. Eprint archive: `arXiv:math.GT/0201243 v2`.

[**Fo53**] Ralph. H. Fox, *Free Differential Calculus I*, Annals of Mathematics **57** (1953), 547-560.

[**Fo96**] Ed Formanek, *Braid group representations of low degree*, Proc. London Math. Soc. **73** (1996), 279-322.

[**FRZ96**] R. Fenn, D. Rolfsen and J. Zhu, *Centralizers in the braid group and singular braid monoid*, L 'Enseignement Math. **42** (1996), 75-96.

[**Fr60**] A. A. Fridman, *On the relation between the word problem and the conjugacy problem in finitely defined groups*, Trudy Moskov, Mat. Obsc. **9** (1960), 329-356.

[**Fr04**] Nuno Franco, *Conjugacy problem for subgroups with applications to Artin groups and braid type groups*, to appear in : Journal of Group Theory, Preprint: `arXiv:math.GR/0411322`

[**FS87**] Amos Fiat and Adi Shamir, *How to Prove Yourself: Practical Solutions to Identification and Signature Problems*, Advances in Cryptology: Proceedings of CRYPTO 86, LNCS **263** (1987), 186-194.

[**Ga61**] Betty Jane Gassner, *On braid groups*, Abh. Math. Sem. Hamburg Univ. **25** (1961), 19-22.

[**Ga69**] Frank A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford (2) **20** (1969), 235-254.

[**Ge94**] Lothar Gerritzen, *Grundbegriffe der Algebra: eine Einführung unter Berücksichtigung funktorieller Aspekte*, Vieweg (1994).

[**Ge05**] Volker Gebhardt, *A New Approach to the Conjugacy Problem in Garside Groups*, Journal of Algebra **292** No.1 (2005), 282-302. Eprint: `arXiv:math.GT/0306199`

[**Ge06**] Volker Gebhardt, *Conjugacy search in braid groups*, Applicable Algebra in Engineering, Communication and Computing **17** (2006), 219-238.

[GG99] Joachim von zur Gathen and Jürgen Gerhard, *Modern Computer Algebra*, Cambridge University Press (1999).

[GG$^+$06] Lothar Gerritzen, Dorian Goldfeld, Martin Kreuzer, Gerhard Rosenberger and Vladimir Shpilrain (Eds.), *Algebraic Methods in Cryptography*, Contemporary Mathematics **418**, AMS (2006).

[GHS06] Anja Groch, Dennis Hofheinz and Rainer Steinwandt, *A Practical Attack on the Root Problem in Braid Groups.* In: L. Gerritzen, D. Goldfeld, M. Kreuzer, G. Rosenberger and V. Shpilrain (Eds.), *Algebraic Methods in Cryptography*, Contemporary Mathematics **418**, AMS (2006), 121-132.

[GK$^+$02] David Garber, Shmuel Kaplan, Mina Teicher, Boaz Tsaban and Uzi Vishne, *Length-based conjugacy search in the braid group*, Preprint (2002): `arXiv:math.GR/0209267`

[GK$^+$05] David Garber, Shmuel Kaplan, Mina Teicher, Boaz Tsaban and Uzi Vishne, *Probabilistic solutions of equations in the braid group*, Advances in Applied Mathematics **35** (2005), 323-334.
Eprint archive: `arXiv:math.GR/0404076`

[GK$^+$06] David Garber, Shmuel Kaplan, Mina Teicher, Boaz Tsaban and Uzi Vishne, *Length-based conjugacy search in the braid group*, In: L. Gerritzen, D. Goldfeld, M. Kreuzer, G. Rosenberger and V. Shpilrain (Eds.), *Algebraic Methods in Cryptography*, Contemporary Mathematics **418**, AMS (2006), 75-87.

[GKT02] David Garber, Shmuel Kaplan and Mina Teicher, *A new algorithm for solving the word problem in braid groups*, Advances in Math. **167**, no. 1 (2002), 142-159. Eprint archive: `arXiv:math.AG/0101053`.

[GM02] R. Gennaro und D. Micciancio, *Cryptanalysis of a Pseudorandom Generator Based on Braid Groups*, Advances in Cryptology - Eurocrypt 2002, LNCS **2332**, Springer (2002), 1-13.

[Go82] J. C. Gower, *Euclidean distance geometry*, The Mathematical Scientist **7** (1982), 1-14.

[Go03] Juan Gonzales-Meneses, *The n-th root of a braid is unique up to conjugacy*, Alg and Geom. Topology **3** (2003), 1103-1118.

[Go05] Juan Gonzales-Meneses, *Improving an algorithm to solve Multiple Simultaneous Conjugacy Problems in braid groups*, Contemporary Mathematics **372** (2005), 35-42. Eprint archive: `arXiv:math.GT/0212150`

[**GP04**] D. Grigoriev and I. Ponomarenko, *Homomorphic public-key cryptosystems over groups and rings*, Quaderni di Mathematica **13** (2004), 305-325. Eprint archive: `arXiv:cs.CR/0309010`

[**Gu88**] G. G. Gurzo, *Systems of generators for centralizers if rigid elements of the braid group*, Izvestiya Mathematics **31**, no. 2 (1988), 223-244.

[**GW04**] Juan Gonzales-Meneses and Bert Wiest, *On the structure of the centralizer of a braid*, Ann. Sci. Ec. Norm. Sup. **37** (2004), 729-757.

[**GZ91**] Max Garzon and Yechezkel Zalcstein, *The complexity of Grigorchuk groups with applications to cryptography*, Theoretical Computer Sciences **88** (1991), 83-98.

[**HEO05**] Derek F. Holt, Bettina Eick and Eamonn A. O'Brien, *Handbook of Computational Group Theory*, Chapman & Hall/CRC (2005).

[**HS03**] Dennis Hofheinz and Rainer Steinwandt, *A Practical Attack on Some Braid Group Based Cryptographic Primitives*, Public Key Cryptography - PKC 2003, LNCS **2567**, Springer (2003).

[**HT02**] J. Hughes and A. Tannenbaum, *Length-based attacks for certain group based encryption rewriting systems*, Workshop SECI02 SEcurité de la Communication sur Internet, Tunis (2002). Updated pdf currently available from: `http://www.storagetek.com/hughes/SECI02.pdf`

[**HT06**] Martin Hock and Boaz Tsaban, *A better length function for Artin's braid groups*, Preprint (2006): `arXiv:math.GR/0611918 v1`

[**Hu67**] Bertram Huppert, *Endliche Gruppen I*, Springer (1967).

[**Hu00**] James Hughes, *The LeftSSS attack on Ko-Lee-Cheon-Han-Kang-Park Key Agreement Protocol in B_{45}*, Presentation, Rump Session CRYPTO 2000, Slides currently available from: `http://www.stortek.com/hughes/Crypt2000.pdf`

[**Hu02**] James Hughes, *A linear algebraic attack on the AAFG1 braid group cryptosystem*, Information Security and Privacy, LNCS **2384**, Springer (2002).

[**Iv04**] Nikolai V. Ivanov, *Examples of Large Centralizers in the Artin Braid Group*, Geometriae Dedicata **105** No.1 (2004), 231-235.

[**Ji86**] Michio Jimbo, *Quantum R-matrix for the generalized Toda system*, Comm. Math. Physics **102** (1986), 537-547.

[**JSI96**] Markus Jakobsson, Kazue Sako and Russell Impagliazzo, *Designated Verifier Proofs and Their Applications*, Advances in Cryptology: Proceedings of EUROCRYPT 96, LNCS **1070** (1996), 143-145.

[**Ka87**] Louis H. Kauffman, *State Models and the Jones Polynomial*, Topology **26** (1987), 395-407.

[**Ka93**] Louis H. Kauffman, *Knots and Physics*, World Scientific, 1993.

[**Ka06**] Arkadius G. Kalka, *Representation attacks on the braid Diffie-Hellman public key encryption*, Applicable Algebra in Engineering, Communication and Computing **17** (2006), 257-266.

[**KC$^+$02**] Ki Hyoung Ko, Doo Ho Choi, Mi Sung Cho and Jang Won Lee, *New Signature Scheme Using Conjugacy Problem*, Cryptology eprint archive: `eprint.iacr.org/2002/168/`.

[**Ki04**] Zeen Kim, *Provably-Secure Identification Schemes based on Conjugacy and DDH Problems*, Master thesis, School of Engineering, Informations and Communications University, Daejon, Korea (2004)

[**KK04**] Zeen Kim and Kwangjo Kim, *Provably-Secure Identification Scheme based on Braid Group*, Proceedings of the 2004 Symposium on Cryptography and Information Security, Sendai, Japan, Jan. 27-30 2004, Volume **1/2**, 29-34. Currently electronically available from:
`http://caislab.icu.ac.kr/Paper/paper_files/2004/SCIS04/scis2004%20-%20zeenkim.pdf`

[**KKL97**] Eon Sook Kang, Ki Hyoung Ko and Sang Jin Lee, *Band-generator presentation for the 4-braid group*, Special issue on Braid Groups and Related Topics, Topology and its Applications **78**, no. 1-2 (1997), 39-60.

[**KL$^+$00**] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang and Choonsik Park, *New Public-key Cryptosystem Using Braid Groups*, Advances in cryptology - CRYPTO 2000, LNCS **1880**, Springer (2000).

[**Ko87**] Neal Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation **48** (1987), 203-209.

[**Ko01**] Ki Hyoung Ko, *Tutorial on Braid Cryptosystem III*,
Currently available from: `knot.kaist.ac.kr/braidcrypt/`.

[**Ko03**] Ki Hyoung Ko, *Conjugacy Problem in Braid Groups and Applications: III. Cryptanalytic approach to conjugacy problem and its variations via representations and linear algebra*, Presentation, 10th school of Knots and Links, University of Tokyo 2003, Talk slides currently available from: `http://kyokan.ms.u-tokyo.ac.jp/~topology/files/KS03b.pdf`

[**Kr00**] Daan Krammer, *The braid group B_4 is linear*, Invent. Math. **142**, no. 3 (2000), 451-486.

[**Kr02**] Daan Krammer, *Braid groups are linear*, Ann. of Math. (2) **155**, no. 1 (2002), 131-156.

[**KT03**] Shmuel Kaplan and Mina Teicher, *Solving the Braid Word Problem Via the Fundamental Group*, In: C. Musili, *Advances in Algebra and Geometry*, Proceedings of University of Hyderabad Conference 2001, Hindustan Book Agency Ltd. (2003).

[**La79**] Gérard Lallement, *Semigroups and Combinatorial Applications*, John Wiley and Sons, New York (1979).

[**La90**] Ruth J. Lawrence, *Homological representations of the Hecke algebra*, Comm. Math. Phys. **135**, no. 1 (1990), 141-191.

[**LC05**] Sunder Lal and Atul Chaturvedi, *Authentication Schemes Using Braid Groups*, Eprint archive: `arXiv:cs/0507066`

[**Le06**] Eonkyung Lee, *Inverting the Burau and Lawrence-Krammer Representations*, In: L. Gerritzen, D. Goldfeld, M. Kreuzer, G. Rosenberger and V. Shpilrain (Eds.), *Algebraic Methods in Cryptography*, Contemporary Mathematics **418**, AMS (2006), 153-160.

[**Le07**] Sang Jin Lee, *Garside groups are strongly translation discrete*, J. Algebra **309** (2007), 594-609.

[**LLH01**] Eonkyung Lee, Sang Jin Lee and Sang Geun Hahn, *Pseudorandomness from Braid Groups*, Advances in Cryptology - Crypto 2001, Proceedings, LNCS **2139**, Springer-Verlag (2001), 486-502.

[**LL02**] Sang Jin Lee and Eonkyung Lee, *Potential weaknesses in the commutator key agreement protocol based on braid groups*, Advances in Cryptology - EUROCRYPT 2002, LNCS **2332**, Springer (2002).

[**Lo89**] Darren D. Long, *On the linear representation of braid groups*, Transactions of the AMS **311** (1989), 535,560.

[**Lo94**] Darren D. Long, *Constructing representations of braid groups*, Communications in Analysis and Geometry, **2**, no. 2 (1994), 217-238.

[**LP93**] D. D. Long and M. Paton, *The Burau representation is not faithful for $n \geq 6$*, Topology **32** (1993), 439-447.

[**LP03**] Eonkyung Lee and Je Hong Park, *Cryptanalysis of the Public-key Encryption based on Braid Groups*, Advances in cryptology - EUROCRYPT 2003, LNCS **2656**, Springer (2003).

[**LT92**] Mirko Lüdde and Francesco Toppan, *Matrix Solutions of Artin's Braid Relations*, Physics Letters B **288**, no. 3-4 (1992), 321-330.

[**L92**] Mirko Lüdde, *Treue Darstellungen der Zopfgruppe und einige Anwendungen*, Dissertation, Mathematisch-Naturwissenschaftliche Fakultät der Rheinischen Friedrich-Wilhelm-Universität, Bonn (1992).

[**L96**] Mirko Lüdde, *Notes on generalised Magnus modules over the braid group*, Mathematische Annalen **306**, no. 1 (1996), 555-569. Preprints Archive of the Sfb 288: Differential Geometry and Quantum Physics, preprint no. 170 (1995), `http://www-sfb288.math.tu-berlin.de/Publications/preprint-list/151/200`

[**Ma39**] Wilhelm Magnus, *On a Theorem of Marshall Hall*, Ann. of Math. **40** (1939), 764-768.

[**Ma47**] A. A. Markov, *On the impossibility of certain algorithms in the theory of associative systems*, I.C.R. (Dokl.) Acad. Sci. URSS **55** (1947), 583-586. (English)

[**Ma68**] G. S. Makanin, engl. translation: *The conjugacy problem in the braid groups*, Soviet Math. Doklady **9** (1968), 1156-1157.

[**Ma71**] G. S. Makanin, *On normalizers in the braid group*, Mat. Sb. **86** (**128**) (1971), 171-179.

[**Ma74**] Wilhelm Magnus, *Braid Groups: A Survey*, Lecture Notes in Mathematics **372**, Springer (1974), 463-487.

[**Ma86**] Yuri Matiyasevitch, *On investigations of some algorithmic problems in algebra and number theory*, Proc. Steklov Inst. Math. **168**, issue 3, Amer. Math. Soc. Translation (1986), 227-252.

[Ma95] Sandro Manfredini, *Some subgroups of Artin's braid group*, Special issue on braid groups and related topics (Jerusalem 1995), Topology Appl. **78**, no. 1-2 (1997), 123-142.

[Ma06a] Samuel Maffre, *A weak key test for braid based cryptography*, Designs, Codes and Cryptography **39**, No.3 (2006), 347-373.

[Ma06b] Samuel Maffre, *Reduction of Conjugacy Problem in Braid Groups, Using Two Garside Structures.* In: Øyvind Ytrehus, *Coding and Cryptography*, Proceedings of the International Workshop WCC 2005, Bergen, Norway, March 2005, LNCS **3696** (2006), 189-201.

[Me28] Karl Menger, *Untersuchungen über alllgemeine Metrik*, Mathematische Annalen **100** (1928), 75-163.

[Me31] Karl Menger, *New foundation of Euclidean geometry*, American Journal of Mathematics **53** (1931), 721-745.

[Me54] Karl Menger, *Géométrie Générale*, Mémorial des Sciences Mathématiques CXXIV, Académie des Sciences de Paris, Gauthier-Villars (1954).

[Mi58] K. A. Mihailova, *The occurence problem for direct products of groups*, Dokl. Akad. Nauk SSSR **119** (1958), 1103-1105. (Russian)

[Mi71] Charles F. Miller III, *On Group-Theoretic Decision Problems and Their Classification*, Annals Math. Studies, No. **78**, Princeton University Press, New Jersey (1971).

[Mi85] V. Miller, *Use of elliptic curves in cryptography*, Advances in cryptology - CRYPTO '85, LNCS **218**, Springer (1985), 417-426.

[Mi99] Jean Michel, *A note on words in braid monoids*, J. Algebra **215**, no. 1 (1999), 366-377.

[MK99] Kunio Murasugi and Bohdan I. Kurpita, *A Study of Braids*, Mathematics and Its Applications **484**, Kluwer Academic Publishers (1999).

[Mo91] John A. Moody, *The Burau representation of the braid group is not faithful for large n*, Bull. Amer. Math. Soc. **25** (1991), 379-384.

[Mo93] John A. Moody, *The faithfulnees question for the Burau representation*, Proc. Amer. Math. Soc. **119** (1993), 439-447.

[Mo94] Lee Mosher, *Mapping Class Groups are Automatic*, Research announcement: Math. Research Letters **1**, no.2 (1994), 249-255.

[Mo95] Lee Mosher, *Mapping Class Groups are Automatic*, The Annals of Mathematics, 2nd Series **142**, no. 2 (1995), 303-384.

[MP69] Wilhelm Magnus and A. Peluso, *On a theorm of V. I. Arnold*, Com. on Pure and Appl. Math. **XXII** (1969), 683-692.

[MST02] S. S. Magliveras, D. R. Stinson and T. van Trung, *New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups*, J. Cryptography **15** (2002), 285-297.

[MSU05] Alexei G. Myasnikov, Vladimir Shpilrain and Alexander Ushakov, *A practical attack on some braid group based cryptographic protocols*, CRYPTO 2005, LNCS **3621** (2005), 86-96.

[MSU06] Alexei G. Myasnikov, Vladimir Shpilrain and Alexander Ushakov, *Random subgroups of braid groups: an approach to cryptanalysis of a braid group based cryptographic protocol*, PKC 2006, LNCS **3958** (2006), 302-314.

[Mu82] Kunio Murasugi, *Seifert fibre spaces and braid groups*, Proc. London Math. Soc. (3) **44** (1982), 71-84.

[Mu87] Jun Murakami, *The Kauffman Polynomial of links and representation theory*, Osaka J. Math. **24** (1987), 745-758.

[Ni86] Jakob Nielsen, In *Collected Papers of J. Nielsen*, Birkhäuser (1986).

[No55] Petr S. Novikov, *On the algorithmic unsolvability of the word problem in group theory*, Trudy Mat. Inst. im. Steklov. **44**, Izdat. Akad. Nauk SSSR, Moscow (1955).

[OOK91] Kazuo Ohta, Tatsuaki Okamoto and Kenji Koyama, *Membership authentication for hierarchical multigroup using the extended Fiat-Shamir scheme*, Advances in Cryptology: Proceedings of EUROCRYPT 90, LNCS **473** (1991), 446-457.

[Or01] Stepan Y. Orevkov, *Quasipositivity test via unitary representations of braid groups and its applications to real algebraic curves*, J. Knot Theory Ramifications **10**, no. 7 (2001), 1005-1023.

[PH$^+$01] S. H. Paeng, K. C. Ha, J. H. Kim, S. Chee and C. Park, *New Public Key Cryptosystem Using Finite Non Abelian Groups*, Advances in Cryptology - Crypto 2001, LNCS **2139**, Springer (2001), 470-485.

[Pi00] Matthieu Picantin, *Petites groupes gaussiens*, Théses de Doctorat de l'Université de Caen (2000).

[Pi01a] Matthieu Picantin, *The conjugacy problem in small Gaussian groups*, Comm. in Algebra **29-3** (2001), 1021-1039.

[Pi01b] Matthieu Picantin, *The center of Garside groups*, Journal of Algebra **245**, no. 1 (2001), 92-122.

[Pi02] Matthieu Picantin, *Explicit presentations for the dual braid monoids*, C. R. Académie Sciences Paris, Série I, **334** (2002), 843-848.
Eprint archive: `arXiv:math.GR/0111280`

[Pi03] Matthieu Picantin, *Automatic structures for torus link groups*, Journal of Knot Theory and its Ramifications **12**, no. 5 (2003), 1-34.
Eprint archive: `arXiv:math.GR/0111079`.

[Pi05] Matthieu Picantin, *Garside monoids vs divisibility monoids*, Mathematical Structures in Computer Science **15**, no. 2 (2005), 231-242.

[PK$^+$01] S. H. Paeng, D. Kwon, K. C. Ha and J. H. Kim, *Improved Public Key Cryptosystem Using Finite Non Abelian Groups*, Cryptology eprint archive: `eprint.iacr.org.2001/066/`.

[Po47] Emil Post, *Recursive unsolvability of a problem of Thue*, J. Symbolic Logic **12** (1947), 1-11.

[PR91] Michael S. Paterson und Alexander A. Razborov, *The set of minimal braids is co-NP-complete*, J. Algorithms **12** (1991), 393-408.

[PZ03] J. Proos and C. Zalka, *Shor's discrete logarithm quantum algorithm for elliptic curves*, Quantum Information and Computation **3** (2003), 317-344.

[Ra79] M. O. Rabin, *Digitized signatures and public-key functions as intractable as factorization*, MIT Laboratory for Computer Science Technical Report, LCS/TR-212 (1979), Currently available from: `www.lcs.mit.edu/publications/pubs/pdf/MIT-LCS-TR-212.pdf`

[RSA78] Ron L. Rivest, Adi Shamir und Leonard Adleman, *A method for obtaining digital signatures and public key cryptosystems*, Communications of the ACM **21** (1978), 120-126.

[Sa01] Bruce E. Sagan, *The Symmetric Group. Representations, Combinatorial Algorihtms and Symmetric Functions*, 2nd Edition, Springer (2001).

[Sc35] Isaac Jacob Schoenberg, *Remarks to Maurice Fréchet's article "Sur la définition axiomatique d'une classe d'espace distanciés vectoriellement applicable sur l'espace de Hilbert "*, Annals of Mathematics **36** (1935), 724-732.

[Sc38] Isaac Jacob Schoenberg, *Metric spaces and positive definite functions*, Transactions of the American Mathematical Society **44** (1938), 522-536.

[SDG06] Herve Sibert, Patrick Dehornoy and Marc Girault, *Entity Authentication Schemes Using Braid Word Reduction*, Discrete Applied Math. **154** (2) (2006), 420-436. Eprint archive: `eprint.iacr.org/2002/187`

[Se65] Jean-Pierre Serre, *Lie algebras and Lie groups*, Benjamin (1965).

[Sh97] Peter Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput. **5** (1997), 1484-1509.

[Si02] Herve Sibert, *Extraction of roots in Garside groups*, Comm. Alg. **30**, no. 6 (2002), 2915-2927.

[SKI90] Hiroki Shizuya, Kenji Koyama and Toshiya Itoh, *Demonstrating possesion without revealing factors and its applications*, Advances in Cryptology: Proceedings of AUSCRYPT 90, LNCS **453** (1990), 273-293.

[SM90] Rani Siromoney and Lisa Mathew, *A public key cryptosystem based on Lyndon words*, Information Proceeding Letters **35** (1990), 33-36.

[So02] Won Taek Song, *The Lawrence-Krammer representation is unitary*, Eprint archive: `arXiv:math.GT/0202214`

[Sq84] Craig C. Squier, *The Burau representation is unitary*, Proc. Amer. Math. Soc. **90**, no. 2 (1984), 199-202.

[St78] V. B. Styšnev, *Taking the root in the braid group*, Izv. Akad. Nauk SSR Ser. Mat. **42**, no. 5 (1978), 1120-1131. (Russian)

[St79] V. B. Styšnev, *The extraction of a root in a braid group*, Izvestiya: Mathematics **13**, no. 2 (1979), 405-416.

[SU05] Vladimir Shpilrain and Alexander Ushakov, *Thompson's group and public key cryptography*, LNCS **3531** (2005), 151-164. Eprint archive: `arXiv:math.GR/0505487`

[SU06a] Vladimir Shpilrain and Alexander Ushakov, *The Conjugacy Search Problem in Public Key Cryptography: Unnecessary and Insufficient*, Applicable Algebra in Engineering, Communication and Computing **17** (2006), 285-289.

[SU06b] Vladimir Shpilrain and Alexander Ushakov, *A new key exchange protocol besed on the decomposition problem.* In: L. Gerritzen, D. Goldfeld, M. Kreuzer, G. Rosenberger and V. Shpilrain (Eds.), *Algebraic Methods in Cryptography*, Contemporary Mathematics **418**, AMS (2006), 161-167.

[SZ06] Vladimir Shpilrain and Gabriel Zapata, *Combinatorial Group Theory and Public Key Cryptography*, Applicable Algebra in Engineering, Communication and Computing **17** (2006), 291-302.

[Ta87] Kay Tatsuoka, *Geodesics in the braid group*, unpublished preprint: Dept. of Math., University of Texas, Austin (1987).

[Th14] Axel Thue, *Probleme über Veränderungen von Zeichenreihen nach gegeben Regeln*, K.V.S.S. No. **10** (1914).

[Th88a] William Thurston, *On the topology and geometry of diffeomorphisms on surfaces*, Bull. AMS **19** (1988), 109-140.

[Th88b] William Thurston, *On the geometry and dynamics of diffeomorphisms on surfaces*, Bull. AMS **19** (1988), 417-431.

[Th92] William Thurston, *braid groups*, chapter 9 in [**EC$^+$92**].

[TL06a] Tony Thomas and Arbind Kumar Lal, *Undeniable Signature Schemes Using Braid Groups*, Eprint archive: `arXiv:cs.CR/0601049` (2006).

[TL06b] Tony Thomas and Arbind Kumar Lal, *Group Signature Schemes Using Braid Groups*, Eprint archive: `arXiv:cs.CR/0602063` (2006).

[Ts05] Boaz Tsaban, *On a authentication scheme based on the root problem in the braid group*, Eprint archive: `arXiv:cs.CR0509059` (2005).

[Tu88] Vladimir Turaev, *The Yang-Baxter equation and invariants of links*, Invent. Math. **92** (1988), 527-553.

[Tu00] Vladimir Turaev, *Faithful Linear Representations of the Braid Groups*, Seminaire BOURBAKI (2000),
Eprint archive: `arXiv:math.GT/0006202`

[**TYM96**] Dian-Min Tong, Shan-De Yang and Zhong-Qi Ma, *A new class of representations of braid groups*, Comm. Theoret. Phys. **26**, no. 4 (1996), 483-486.

[**Wa67**] F. Waldhausen, *Gruppen mit Zentrum und 3-dimensionale Mannigfaltigkeiten*, Topology **6** (1967), 505-517.

[**We90**] Hans Wenzl, *Quantum groups and subfactors of type B, C and D*, Comm. Math Phys. **133** (1990), 383-432.

[**Wi02**] Bert Wiest, *An algorithm for the word problem in braid groups*, Eprint archive: `arXiv:math.GT/0211169` (2002).

[**WM85**] Neal R. Wagner und Marianne R. Magyarik, *A public key cryptosystem based on the wordproblem*, Advances in Cryptology, Proceedings of Crypto '84, LNCS **196**, Springer-Verlag (1985), 19-36.

[**Xu92**] Peijun Xu, *The genus of closed 3-braids*, J. Knot Theory and its Ramifications **1**, no.3 (1992), 303-326.

[**Zh06**] Hao Zheng, *A New Approach to Extracting Roots in Garside Groups*, Communications in Algebra **34**, no. 5 (2006), 1793-1802.

[**Zi01**] Matthew G. Zinno, *On Krammer's representations of the braid groups*, Math. Ann. **321**, no. 1 (2001), 197-211. Eprint archive: `arXiv:math.RT/0002136`

[**ZZQ06**] Zou Shi-hua, Zeng Ji-wen and Quan Jun-jie, *Designated Verifier Signature Scheme Based on Braid Groups*, Cryptology eprint archive: `eprint.iacr.org/2006/329`