ISSN 1346−7387

JOURNAL OF MATHEMATICS
THE UNIVERSITY OF TOKUSHIMA

VOLUME 39
2005

PUBLISHED BY THE
UNIVERSITY OF TOKUSHIMA
TOKUSHIMA, JAPAN

CONTENTS

ISHIHARA, T. : Local Switching of Signed Induced Cycles ···················· 1

YASUI, H. and KATAYAMA, S. : Maps $R:\mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{Z}/n^2\mathbf{Z}$ and Some Cryptographic Applications ·· 7

KUWABARA, R. : A Geometrical Formulation for Classical Mechanics in Gauge Fields ·· 23

J. Math. Univ. Tokushima
Vol.39 (2005), 1-5

Local Switching of Signed Induced Cycles

By

Toru ISHIHARA

Faculty of Integrated Arts and Sciences,
The University of Tokushima,
Minamijosanjima, Tokushima 770-8502, JAPAN
e-mail adress: ishihara@ias.tokushima-u.ac.jp

(Received September 30, 2005)

Abstract

A singed cykle is transformed to a line by a sequence of local switchings if and only if its parity is odd. We invesigate induced cycles in a signed graph which are transformed to lines by local switching.

2000 Mathematics Subject Classification. 05C22

Introduction

Local switching of signed graphs is introduced by P. J. Cameron, J.J. Seidel and S. V. Tsaranov in [2]. Signed cycles with odd parity are transformed to lines by a sequence of local switchings, but signed cycles with even parity can not be transformed to lines by no means [5]. What kinds of induced signed cyles are transformed to trees by a sequence of local switchings ? We investigate induced cycles in a signed graph which are transformed into lines by local switching.

We state briefly basic facts about signed graphs. A graph $G = (V, E)$ consists of an n-set V(the vertices) and a set E of unordered pairs from V(the edges). A *signed graph* (G, f) is a graph G with a signing $f : E \to \{1, -1\}$ of the edges. We set $E^+ = f^{-1}(+1)$ and $E^- = f^{-1}(-1)$. For any subset $U \subseteq V$ of vertices, let f_U denote the signing obtained from f by reversing the sign of each edge which has one vertex in U. This defines on the set of signings an equivalence relation, called *switching.* The equivalence classes $\{f_U : U \subseteq V\}$ are the *signed swithing classes* of the graph $G = (V, E)$.

Let $i \in V$ be a vertex of G, and $V(i)$ be the neighbours of i. The *local graph* of (G, f) at i has $V(i)$ as its vertex set, and as edges all edges $\{j, k\}$ of G for which $f(i, j)f(j, k)f(k, i) = -1$. A *rim* of (G, f) at i is any union of connected components of local graph at i. Let J be any rim at i, and let $K = V(i)\backslash J$. *Local switching* of (G, f) with respect to (i, J) is the following operation:(i) delete all edges of G between J and K; (ii) for any $j \in J$, $k \in K$ not previously joined, introduce an edge $\{j,k\}$ with sign chosen so that $f(i,j)f(j,k)f(k,i) = -1$; (iii) change the signs of all edges from i to J; (iv) leave all other edges and signs unaltered. Let Ω_n be the set of switching classes of signed graphs of order n. Local switching , applied to any vertex and any rim at the vertex, gives a relation on Ω which is symmetric but not transitive. The equivalence classes of its tansitive closure are called the *clusters* of order n.

A signed graph is said to be *positive* if we can switch all signs of its edges into +1. A tree is always considered as a positive signed graph. A tree with only two leaves is said to be *a line* in the present paper.

1. Signed induced cycles

A $k-$cycle $C^k = (V, E)$, where $V = \{a_1, a_2, \cdots, a_k\}$, $E = \{a_1a_2, a_2a_3, \cdots, a_{k-1}a_k, a_ka_1\}$, will be denoted simply $C^k = a_1a_2 \cdots a_ka_1$. For signed cycles, there are two switching classes, which are distinguished by the parity or the balance, where the parity of a signed cycle is the parity of the number of its edges which carry a positive sign and the balance is the product of the signs on its edges [2]. We show the follwing in [5].

Theorem . *Let C^k be a $k-$cycle. Then, it is transformed to a tree by a sequence of local switchings if and only if its parity is odd.*

In the present note, we study induced cycles in a signed graph which are transformed into lines by local switching.

An induced cycle with odd (resp. even) parity in a signed graph is called simply an *odd* (resp. *even*) induced cycle in the present paper. Let C be an induced cycle in a signed graph. Let P be a path between vetices a and b which are vertices of C. We call P a *C-path* if P meets C exactly in its ends, and in this case we call it also *a-b path.*

Theorem 1. *Let C be an induced cycle in a signed graph G. For some two its vertices a, b, suppose that there is a C-path P between a and b. Together with two pathes P_1, P_2 between a and b in C, P forms two induced cycles C_1 and C_2. If C is an odd induced cycle, then one of C_1 and C_2 is odd , and the other is even. On the other hand, if C is even, both of C_1 and C_2 are even or odd.*

Proof. Now a parity of a signed path is defined to be the parity of the numbers of positive edges. Firstly, suppose that C is an odd induced cycle. Then, the parity of one of two pathes P_1 and P_2 is odd and the parity of the other is even. We may assume that P_1 is an odd path. Then P_2 is an even path. If P is an odd(resp. even) path, then C_1 is an even(resp. odd) cycle and C_2 is an odd(resp. even) cycle.

Next, suppose that C is an even induced cycle. Then both P_1 and P_2 are odd pathes or even pathes. Suppose that P_1 and P_2 are odd pathes. If P is an odd(resp. even) path, both C_1 and C_2 are even(resp. odd) induced cycles.

When P_1 and P_2 are even pathes, if P is an odd(resp. even) path, both C_1 and C_2 are odd(resp. even) induced cycles.

The following is evident.

Proposition 2. *Let C be an induced cycle in a signed graph G with length k. Take any vertex a of C. Let C' be the induced cycle obtained from C by local switching at a. Then C' has the same parity as C and its length is $k-1$.*

Definition 1. For a given induced cycle C, take any C-path P. As in Theorem 1, we can construct two cycles C_1, C_2. In this case, we say that C *consists of* C_1 and C_2 and that C_1 and C_2 are contained in C. Assume that C is even. If C_1, C_2 are odd, we say that C *consists of odd cycles.* If C_1, C_2 are even but they consist of odd cycles, we say also C *consists of odd cycles.* If C_1, C_2 are even , C_1 consists of odd cycles and C_2 consists of two cycles C_{21}, C_{22} which consist of odd cycles, we say also C *consists of odd cycles* and so on.

Definition 2. Let C be an induced cycle in a signed graph.

We call C a *fundamental odd cycle* if the following two conditions are satisfied. (1) Its parity is odd. (2) If C consists of two induced cycles C_1, C_2 and C_1 is odd, then the even cycle C_2 does not consists of odd cycles. We call C a *fundamental even cycle* if the following tree conditions are satisfied. (1) Its parity is even.(2) It does not consists of odd cycles. (3) For any vertices a, b of C, there is no $a-b$ path whose length is shoter than the lengthes of two $a-b$ pathes on C. The following is evident.

2. Local swithching of signed induced cycles

Lemma 3. *Let C be an induced cycle in a signed graph G with length k. Take a vertex d in the outside of C which is adjacent to vertices a, b of C, where ab is one of the edges of C. Moreover suppose there is no other vertex of C which is adjacent to d. Let C' be the induced cycle obtained from C by local switching at d. Then C' has the same parity as C and its length is $k+1$.*

Let C be a fundamental even cycle in a signed graph G. Take a vertex d in the oudside of C. Assume that the vertex v is adjacent to some vertices of C. The following three cases may occur. (1) There is an edge ab of C and vertices of C which are adjacent to v are just a, b. As C is a fundamental even cycle, there is no pathes which link the vertex v and any other vertice of C. (2) Edges ab and bc are contained in C and vertices of C which are adjacent to v are just a, c or (3) a, b, c. Since C is a fundamental cycle, we have no other cases. When the case (1) occurs, by local switching at d, we get an even cycle C_1 with length one longer than that of C. If there is a C-path which links a and b and makes a fundamental odd cycles with $a-b$ pathes in C, then C consists of odd cycles and is not a fundamental even cycle. Thus, C_1 is a fundamental even cycle. For case (2), by local switching at v, we get two fundamental even cycle *abca* and the cycle consist of the edge ac and the other $a-c$ path in C. The length of the latter is one less than that of C. In the case (3), suppose that C consists of the path abc and the other $a-c$ path P. By local switching at d, we obtain a fundamental even cycle C_1 which consists of the edge ac and the path P and has the length one less than that of C, or a even cycle C_2 which consists of the path adc and the path P. As C is a fundamental even cycle, C_2 is also a fundamental even cycle with the same length as that of C.

Summing up, we have

Lemma 4. *Let C be a fundamental even cycle in a signed graph G.*

(1) Take any vertex a in C. By local switching at a, we get a fundamental even cycle with lengh one less than that of C. Take a vertex v outside C which is adjacent to some vertices in C. Then the following two cases occur.

(2) Edges ab and bc are contained in C and vertices of C which are adjacent to the vertx v are just a, c or a, b, c. By local swithing at v, we get a fundamental even cycle with lengh one less than that of C or with the same length as that of C.

(3) There is an edge ab of C and vertices of C which are adjacent to v are just a, b. By local switching at d, we get an even induced cycle C_1 with length one longer than that of C. This C_1 may consists of odd cycles. Otherwise, C_1 is a fundamental even cycle.

Let C be a fundamental odd cycle in a signed graph G. Take a vertex d in the outside of C. Assume that the vertex v is adjacent to vertices a, b of C and that ab is an edge of C. As C is a fundamental odd cycle, there are no pathes which link the vertex v with any other vertices of C, By local swithing at v, we obtain a fundamental odd cycle with lengh one longer than that of C. Assume only two vertices a, b of C are adjacent to v and that a, b are not adjacent. Suppose that signs of the edges av and bv are positive. Then, one of $a-b$ path P in C is an even path. The path adb and P make an even cycle. By local switching at v, we get an fundamental even cycle with length less than that of C. Let $a_1, a_2, \cdots, a_k$ be vertices of C which are adjacent to v. We may assume that these vertices are on C in this order and that signs of the edges $va_1, va_2, \cdots, va_k$ are positive. We may also suppose that all pathes $a_1 - a_2$ path, $a_2 - a_3$ path, $\cdots$ $a_{k-1} - a_k$ path are even pathes. By local switching at v, we get at least $k-1$ fundamental even cycles with length less than that of C.

Lemma 5. *Let C be a fundamental odd cycle in a signed graph G.*

(1) Take any vertex a in C. By local switching at a, we get a fundamental odd cycle with lengh one less than that of C.

Take a vertex v outside C which is adjacent to some vertices in C. Then the following two cases occur.

(2) There is an edge ab of C and vertices of C which are adjacent to v are just a, b. By local switching at d, we get a fundamental odd cycle C_1 with length one longer than that of C.

(3) The vertex v is adjacent to some vertices in C any two of which are not adjacent. By local swithing at v, we obtain at least one fundamental even cycle with length less than that of C.

Theorem 6. *We list some facts about transforming cycles into lines by a sequence of local switichings.*

(1) A cycle with length longer than three is not able to be transformed into a line by a local switching. Only an odd cycle with length three can be toransformed into a line by a local switching.

(2) A fundamental even cycle C can not be transformed into line by a sequence of local switchings when it remains as an even cycle. If there is a vertex v outside C and it is adjacent to only two vertices a, b in C where ab is an edge of C, by local switching at v, we obtain an even cycle with length one longer than that of C. Moreover if this cycle consisits of odd cycles, it may be trannsformed into a line by a sequence of local switchings.

(3) The outside vertex v is adjacent to some vertices in C any two of which are not adjacent. Scince by local switching at v, we obtain some fundamental even cycles, we must avoid this local switching in order to transform the cycle into a line.

Example 1. Let $G = (V, E)$ be a signed graph with $V = \{a_1, a_2, a_3, a_4, a_5\}$ and $E^+ = \{a_1a_2, a_2a_3, a_3a_4, a_3a_5, a_4a_1\}$, $E^- = \{a_1a_5\}$. An even cycle $a_1a_2a_3a_4a_1$ consists of two odd cycles $a_1a_2a_3a_5a_1$ and $a_1a_5a_3a_4a_1$. As a_2 and a_4 are regarded inner vertices of the even cycle, by local switching at a_2 or a_4, we obtain an even 3-cycle. On the other hand, by local switching at a_5, we get three odd 3-cycles. By local switching with respect to $(a_1, J = \{a_2\})$, we get an even 3-cycle, because it is regarded as local switching at an inner vertex of an even cycle. On the other hand, by local switching with respect to $(a_1, J = \{a_2, a_4\})$, we obtain odd 3-cycles.

References

[1] P. J. Cameron, J. M. Goethals, J. J. Seidel and E. E. Shult Line graphs, root systems, and Elliptic geometry, J. Algebra, **43**(1976), 305-327.

[2] P. J. Cameron, J. J. Seidel and S. V. Tsaranov, Signed Graphs, Root lattices, and Coxeter groups, J. Algebra, **164**(1994), 173-209.

[3] T. Ishihara, Signed Graphs Associated with the Lattice A_n, J. Math. Univ. Tokushima, **36**(2002), 1-6.

[4] T. Ishihara, Local Switching of Some Signed Graphs, J. Math. Univ. Tokushima, **38**(2004), 1-7.

[5] T. Ishihara, Local Switching, Hushimi tree and tree, to appear.

J. Math. Univ. Tokushima
Vol.39 (2005), 7-21

Maps $R : Z/nZ \longrightarrow Z/n^2Z$ and Some Cryptographic Applications

By
Hiroharu YASUI and Shin-ichi KATAYAMA

Kurayoshi-higashi High School, Kurayoshi, Tottori, 682-0812, JAPAN
and
Department of Mathematical and Natural Sciences, Faculty of Integrated Arts and Sciences, The University of Tokushima, Tokushima 770-8502, JAPAN
e-mail address : hiroharu1979@yahoo.co.jp
: katayama@ias.tokushima-u.ac.jp

(Received September 30, 2005)

Abstract

In his master thesis [8], the first author has studied the RSA signatures with several types of redundancy functions. In this paper, we shall introduce these redundancy functions and investigate arithmetic properties of these redundancy functions and the signatures with these redundancy functions.

2000 Mathematics Subject Classification. Primary 11N45; Secondary 11A07, 94A62

Introduction

The purpose of this paper is to generalize the digital signatures with redundancy functions introduced in [8] and investigate arithmetic properties of these redundancy functions and the signatures with these redundancy functions.

Firstly, we briefly describe the RSA signature scheme. Let n be the product of randomly chosen distinct large primes p and q. Then the message space and the cipher text space for the RSA public-key encryption scheme are both Z/nZ. The RSA signature scheme can be created by reversing the roles of the encryption and the decryption as follows.

We denote Alice's public key and secret key by e and d, respectively. Note that the public key and the secret key satisfy $ed \equiv 1 \ mod \ \varphi(n)$. Here φ is the

Euler's φ function and satisfies $|(Z/nZ)^\times| = \varphi(n)$.
Alice can sign any message $m \in (Z/nZ)^\times$ by applying her secret key d

$$s \equiv m^d \in (Z/nZ)^\times.$$

Bob can check the signature by applying Alice's public key e, i.e.,

$$s^e \equiv m^{de} \equiv m \ mod\ n.$$

We will explain the reason why this is a signature. By raising the randomly looking number to the power e, one may recover the plain text m. Hence s can be considered to the eth root of m and computing eth roots of an integer $m\ mod\ n$ without the knowledge of d is infeasible. Since Alice is the only one who knows d, Bob can verify that Alice must have computed s and thereby signed m. We note that any one who knows Alice's Public key (n, e) can also verify this signature s.

Though the original idea of the RSA signature is the one described as above, there are a number of possible attacks. We explain here some of those attacks.

Firstly, we shall explain the *existential forgery.* Oscar chooses $s \in (Z/nZ)^\times$ and claims that s is a RSA signature of Alice. If $m = s^e\ mod\ n$ is a meaningful text, one believes that Alice has signed m. This is called an *existential forgery.*

Another attack comes from the fact RSA is multiplicative. Let $m_1, m_2 \in (Z/nZ)^\times$ and their signatures are $s_1 \equiv m_1^d\ mod\ n$ and $s_2 \equiv m_2^d\ mod\ n$. Put $m = m_1m_2\ mod\ n$. Then

$$s = s_1s_2 \equiv m_1^dm_2^d = (m_1m_2)^d \equiv m^d\ mod\ n.$$

Thus s is the signature of the message m. This is called a *multiplicative attack.*

There are two known methods to protect from these attacks. The first one is to use the *hash function h* and the second one is to use the *redundancy function*

$$R : Z/nZ \longrightarrow Z/nZ.$$

In order to protect from the *multiplicative attack*, it is important that the redundancy function R is not multiplicative. Moreover it should be expected R satisfies the following property.

For any $x, y \in Z/nZ$,

$$R(x)R(y) \not\equiv R(z)\ mod\ n \quad \text{for any } z \in Z/nZ.$$

In [1] 11.2.5, a redundancy function based on the binary expansion of x $(0 < x < n)$ was proposed. It seems that two attacks described above no longer work for the signature with this redundancy function, but we could not verify it mathematically.

Thus, instead of these usual redundancy functions $R : Z/nZ \longrightarrow Z/nZ$, the first author introduced other redundancy functions

$$R : Z/nZ \longrightarrow Z/n^2Z$$

and studied the security of the signatures with these new redundancy functions. In the following, we shall introduce these redundancy functions and study the arithmetic properties of these redundancy functions.

1. Redundancy functions R_k and arithmetical properties

In the following, we shall introduce several redundancy functions and investigate the fundamental properties of these redundancy functions.
Let k be any fixed natural number ≥ 2. We shall introduce a redundancy function $R_k : \{0, 1, \cdots, n-1\} \to \{0, 1, \cdots, n^k - 1\}$ by putting

$$R_k : w \mapsto R_k(w) = \overbrace{w \circ w \circ \cdots \circ w}^{k}.$$

Here, for any $0 \leq w < n$, we denote $wn^{k-1} + wn^{k-2} + \cdots + w \ mod\ n^k$ by

$$w \circ w \circ \cdots \circ w.$$

In the following, we shall consider the conditions of (x, y) when $R_k(x)R_k(y) \equiv R_k(z)$ for some z. Firstly, we shall show it is rare to occur $R_2(x)R_2(y) \equiv R_2(z)$. Finally, we shall show that $R_k(x)R_k(y) \not\equiv R_k(z)$ for any $k \geq 3$.

Consider the case when n is any natural number and $k = 2$. It is obvious that $(0 \circ 0)(x \circ x) = 0 \circ 0$ for any $x \in Z/nZ$. Thus, in the following, we shall restrict ourselves to non-trivial cases $0 < x, y < n$.
We call

(x, y) $(1 \leq x, y < n)$ has the *double structure*

if

$$(x \circ x)(y \circ y) \equiv z \circ z \ \ mod\ n^2 \ \text{ for some } z.$$

Then we have the following fundamental lemma.

Lemma 1. *(x, y) has the double structure if and only if*

$$x \cdot y = an + n - a, \quad \textit{with some } a \ (0 < a < n).$$

Proof. Put $x \cdot y = an + b \quad (0 \leq a, b < n)$. Then we have

$$\begin{aligned} (xn + x)(yn + y) &= xy(n^2 + 2n + 1) \\ &= (an + b)(n^2 + 2n + 1) \\ &\equiv (an + b)(2n + 1) \ mod\ n^2 \\ &\equiv (a + 2b)n + b \ \ mod\ n^2. \end{aligned}$$

Then

$$(x, y) \text{ has the double structure} \iff a + 2b \equiv b \quad \mathit{mod}\ n$$
$$\iff a + b \equiv 0 \quad \mathit{mod}\ n.$$

Since $0 < a + b \leq 2n - 2$, we have

$$n|(a + b) \iff a + b = n.$$

Thus we have shown

$$(x, y) \ \text{ has the double structure } \iff a + b = n.$$

Thus we have completed the proof.

Let G be the multiplicative group of residues modulo $n - 1$, i.e., $(Z/(n - 1)Z)^{\times}$. If any x with $1 \leq x < n$ satisfies $x|n$, then we see that $x \cdot (n/x) = n \equiv 1 \ \mathit{mod}\ (n - 1)$. Hence we can define a subset H of G by putting

$$H = \{x \ \mathit{mod}\ n \mid 1 \leq x < n \text{ with } x|n\}.$$

We note that $|G| = \varphi(n - 1)$ and $|H| = d(n) - 1$, where φ is the Euler's function and d is the divisor function.

Lemma 2. *(x, y) has the double structure if and only if*

$$x \not| n \ \mathit{and} \ \ y \equiv x^{-1} \ \mathit{mod}\ (n - 1).$$

Proof. From Lemma 1, we know that (x, y) has the double structure if and only if $xy = an + n - a$ with $0 < a < n$. We see $an + n - a = a(n - 1) + n \equiv 1 \ \mathit{mod}\ (n - 1)$. Thus we know if (x, y) has the double structure, then $y \equiv x^{-1} \ \mathit{mod}\ (n - 1)$. Moreover $a \neq 0$ implies $x \not| n$.

Conversely, assume $x \in G - H$ and put $y \equiv x^{-1} \ \mathit{mod}\ (n - 1)$ with $0 < y < n$. Then one can write

$$xy = b(n - 1) + 1 = bn - b + 1 = (b - 1)n + n - (b - 1) \quad \text{with some } 0 \leq b < n.$$

From the assumption $x \notin H$, we see $x \not| n$, i.e., we have $b \neq 0, 1$. Thus we have $0 < b - 1 < n$, which means that (x, y) has the double structure. Hence we have shown

$$(x, y) \text{ has the double structure}$$
$$\iff x \in G - H \ \text{ and } y \equiv x^{-1} \ \mathit{mod}\ (n - 1)$$
$$\iff x \not| n \text{ and } \ y \equiv x^{-1} \ \mathit{mod}\ (n - 1).$$

Let $K(n)$ be the number of the pairs (x, y) with $0 < x, y < n$ which have the double structure. Then, from the above lemmas, $K(n)$ equals to the number of the elements contained in the set $G - H$. Hence we have shown the following theorem.

Theorem 1.

$$K(n) = \varphi(n-1) - d(n) + 1.$$

We note that we can estimate the security of the RSA signature with the redundancy function R_2 from the multiplicative attack by estimating the ratio of the following numbers:

$$\frac{\text{the number of the pairs } (x,y) \text{ which has the double structure}}{\text{the number of all the pairs } (x,y)} = \frac{K(n)}{(n-1)^2}.$$

In the following, we shall show

$$\frac{K(n)}{(n-1)^2} \longrightarrow 0, \quad \text{as } n \longrightarrow \infty.$$

More precisely, we shall show

$$\frac{\log(K(n))}{\log(n-1)} \longrightarrow 1, \quad \text{as } n \longrightarrow \infty.$$

Firstly, we have to estimate $\varphi(n-1)$. It is obvious that for any $n > 2$, $\varphi(n-1) < n-1$. Moreover one can easily show the following:

Lemma 3. (Hatalová and T. Šalát [3]) *For any $n \geq 4$,*

$$\frac{\log 2}{2} \times \frac{n-1}{\log(n-1)} < \varphi(n-1) < n-1$$

Proposition 1. *$K(n)$ satisfies the following inequality*

$$\begin{aligned} K(n) &> \frac{(n-1)\log 2}{2\log(n-1)} - 2\sqrt{n} \\ &> \frac{(n-1)\log 2}{4\log(n-1)} \qquad (n > 11688) \end{aligned}$$

Proof. Firstly we note the smaller one of the divisor a of n must satisfies the inequality $a \leq \sqrt{n}$. Thus we know

$$d(n) - 1 < 2\sqrt{n}.$$

Next, we shall show $\dfrac{(n-1)\log 2}{4\log(n-1)} > 2\sqrt{n} \quad (n > 11688)$.

We define a function $f(n)$ by putting

$$\begin{aligned} f(n) &= \frac{(n-1)\log 2}{4\log(n-1)} - 2\sqrt{n} \\ &= \frac{(n-1)\log 2 - 8\sqrt{n}\log(n-1)}{4\log(n-1)}. \end{aligned}$$

Put

$$g(n) = (n-1)\log 2 - 8\sqrt{n}\log(n-1).$$

Then

$$\begin{aligned} g^{'}(n) &= \log 2 - \frac{4\log(n-1)}{\sqrt{n}} - \frac{8\sqrt{n}}{n-1} \\ &\to \log 2 > 0 \quad (n \to \infty). \end{aligned}$$

Now we can easily verify $f(11687) = -0.00553\cdots, f(11688) = 0.00173\cdots$ and $f'(n) > 0$ for $n > 11688$. Thus we have completed the proof.

From this proposition, for any $n > 11688$, we have

$$\log(K(n)) > \log(n-1) - \log\log(n-1) + \log\log 2 - \log 4.$$

Since it is obvious that $\log(K(n)) < \log(n-1)$, we have shown the security of the RSA signatures with this redundancy function R_2 against the multiplicative attack as follows.

Theorem 2.

$$\lim_{n\to\infty} \frac{\log K(n)}{\log(n-1)^2} = \frac{1}{2}.$$

Finally we shall consider the cases $k > 2$. Assume $0 < x, y < n$ satisfies

$$R_{k+1}(x)R_{k+1}(y) \equiv R_{k+1}(z) \ mod \ n^{k+1} \text{ for some } z \ (0 < z < n).$$

Then, from the fact $R_{k+1}(x) \equiv R_k(x) \ mod \ n^k$, (x, y) also satisfies

$$R_k(x)R_k(y) \equiv R_k(z) \ mod \ n^k.$$

Now we shall show the following lemma.

Lemma 4. *For any $0 < x, y, z < n$, we have*

$$R_3(x)R_3(y) \not\equiv R_3(z) \ mod \ n^3.$$

Proof. Assume, on the contrary

$$R_3(x)R_3(y) \equiv R_3(z) \ mod\ n^3 \text{ for some } z.$$

Then

$$R_2(x)R_2(y) \equiv R_2(z) \ mod\ n^2.$$

Hence, from Lemma 1, x, y satisfies $xy = an + n - a$ with some a $(0 < a < n)$. Therefore

$$\begin{aligned} R_3(x)R_3(y) &= (an+n-a)(n^2+n+1)^2 \equiv (an+n-a)(3n^2+2n+1) \\ &\equiv (n-a+1)n^2 + (n-a)n + n - a \\ &\equiv (n-a+1) \circ (n-a) \circ (n-a) \ mod\ n^3. \end{aligned}$$

We see that $(n-a+1) \circ (n-a) \circ (n-a) \neq z \circ z \circ z$, which completes the proof.

From this lemma and the relations of R_k and R_{k+1} described as above, we see

$$R_k(x)R_k(y) \not\equiv R_k(z) \ mod\ n^k \text{ for any } k \geq 3.$$

Thus we have shown:

Theorem 3.

$$R_k(x)R_k(y) \not\equiv R_k(z) \ mod\ n^k, \ \textit{for any } k \geq 3.$$

Remark 1. If we use the RSA signature with the redundancy function R_3, it takes about 27 times to generate and verify this signature compared to the usual signature. But we think this RSA signature is of interest, because, from this theorem, the multiplicative attack can no longer be applied to this signature.

2. On the structure of $K(n)$ and H

In this section, we shall consider the arithmetic properties of $K(n)$ and H more precisely. Though we don't use this property later, we think it is worth for studying the structure of H here. Firstly, we shall consider the special case $n = 2^r$. Here we shall give a table of the numbers $K(2^r)$ for small r.

r	$(2^r-1)^2$	$K(2^r)$
2	9	0
3	49	3
4	225	4
5	961	25
6	3969	30
7	16129	119
8	65025	120
9	261121	423
10	1046529	590
11	4190209	1925
12	16769025	1716
13	67092481	8177
14	268402689	10570
15	1073676289	26985
16	4294836225	32752
17	17179607041	131053

Table 1: Calculations of the number $K(2^r)$ using UBASIC86

From this table, we see $r|K(2^r)$ for small r. Actually, we can show $K(2^r)$ has the following property.

We shall define the maps σ and σ^{-1} on $K(2^r)$ by putting

$$\sigma=\begin{cases} x\longmapsto 2x & (1\le x\le 2^{r-1}-1)\\ x\longmapsto 2(x-2^{r-1})+1 & (2^{r-1}\le x\le 2^r-1)\end{cases}$$

$$\sigma^{-1}=\begin{cases} y\longmapsto \dfrac{y}{2} & (y=2k,k\in N)\\ \\ y\longmapsto \dfrac{y-1}{2}+2^{r-1} & (y=2k+1,k\in N)\end{cases}$$

Since

$$\sigma(x)\sigma^{-1}(y)=xy,$$

we can define a map $\tilde{\sigma}$ on $K(2^r)$, by putting

$$\tilde{\sigma}:(x,y)\longmapsto(\sigma(x),\sigma^{-1}(y)).$$

Example of $\tilde{\sigma}$ for the case $r = 6$.

$$\begin{tikzcd}
& (000101,100110) \arrow[r, "\tilde{\sigma}"] & (001010,010011) \arrow[dr, "\tilde{\sigma}"] & \\
(100010,001101) \arrow[ur, "\tilde{\sigma}"] & & & (010100,101001) \arrow[dl, "\tilde{\sigma}"] \\
& (010001,011010) \arrow[ul, "\tilde{\sigma}"] & (101000,110100) \arrow[l, "\tilde{\sigma}"] &
\end{tikzcd}$$

In [8], the first author proved this map has the order r using only the elementary argument, i.e., he proved that, for any $0 < d(1) < d(2) \leq r$,

$$\tilde{\sigma}^{d(1)}((x,y)) \neq \tilde{\sigma}^{d(2)}((x,y))$$

and

$$\tilde{\sigma}^{r}((x,y)) = (x,y).$$

In this paper, we shall give another proof based on the structure of the group G. From the definition, we see that, for any $n = 2^r$,

$$H = \{x \ mod \ n(= 2^r) | 1 \leq x < n \text{ and } x|n\} = \{1, 2, 4, \dots, 2^{r-1} \ mod \ 2^r\}.$$

Thus H is the subgroup $\langle 2 \rangle$ of $G = (Z/nZ)^\times$ for this case $n = 2^r$. We can verify the map $\tilde{\sigma}$ on $K(2^r)$ is nothing but dividing the set $G - H$ into the cossets of H in G. Since $|H|$(= the order of 2 mod 2^r) $= r$, we have shown $r|K(2^r)$.

Let ℓ be a prime. Consider the case $n = \ell^r$. Then, in the same way as above, we see $H = \langle \ell \rangle < G$ and $|H|$(= the order of ℓ mod ℓ^r) $= r$ and $r|K(\ell^r)$.

Conversely, we shall show that $H < G$ implies $n = \ell^r$ for some prime ℓ. Assume $H < G$. Let ℓ be the smallest prime which divides n. From the condition $\ell|n$, we see $\ell \ mod \ n \in H$. The assumption $H < G$ implies any powers of $\ell \ mod \ n$ must be contained in H. If n is not the power of primes, then there exist $r > 0$ with $\ell^r|n$ but $\ell^{r+1} \not| \ n$ and $\ell^{r+1} < n$. Thus $\ell^{r+1} \ mod \ n \notin H$, which is the contradiction.

Therefore we have shown the following theorem.

Theorem 4. *With the above notation,*

$$H < G \iff n = \ell^r \text{ with some prime } \ell.$$

Moreover, we have $r|K(\ell^r)$.

3. Other redundancy functions

In the following, we shall investigate other redundancy functions. Let t be a fixed non-negative integer. We define a redundancy function $R_{(to1)}$ by putting

$$R_{(t\circ 1)} : \{0, 1, \cdots, n-1\} \to \{0, 1, \cdots, n^2 - 1\}\ ,\ w \mapsto R_{(t\circ 1)}(w) = t \cdot w \circ w.$$

Here we denote $twn + w\ mod\ n^2$ by $tw \circ w$. We shall call

$$(x, y) \text{ has the } (t \circ 1) \textit{ structure}, \text{ if}$$

$$R_{(t\circ 1)}(x)R_{(t\circ 1)}(y) \equiv R_{(t\circ 1)}(z)\ mod\ n^2 \quad \text{for some } z\ (0 < z < n).$$

Let $K_{(t\circ 1)}(n)$ be the number of the elements (x, y) which have the $(t \circ 1)$ structure. Let us denote $xy = an + b$ with $0 \leq a, b < n$, then we see

$$R_{(t\circ 1)}(x)R_{(t\circ 1)}(y) \equiv (an + b)(2tn + 1) \equiv (a + 2tb)n + b\ mod\ n^2.$$

Thus

$$(x, y) \text{ has the } (t \circ 1) \text{ structure} \Longleftrightarrow a + tb \equiv 0\ mod\ n.$$

Since $0 < a, b < n$, we see

$$a + tb \equiv 0\ mod\ n \Longleftrightarrow a + tb = n, 2n, \ldots, tn.$$

Thus we can estimate

$$K_{(t\circ 1)}(n) \leq tn$$

and

$$\limsup_{n\to\infty} \frac{\log(K_{(t\circ 1)}(n))}{\log(n-1)^2} \leq \frac{1}{2} \quad \text{for any fixed } t.$$

We note that the redundancy function R_2 investigated in Section 1 is the special case $R_{(1\circ 1)}$. In general, we have the following weak but generalized results.

Theorem 5. *With the above notation, we have*

$$\limsup_{n\to\infty} \frac{\log(K_{(t\circ 1)}(n))}{\log(n-1)^2} \leq \frac{1}{2},$$

In [8], the first author investigated the cases $t = 2$ and 3 more precisely and conjectured that, for any odd n,

$$\lim_{n\to\infty} \frac{\log(K_{(t\circ 1)}(n))}{\log(n-1)^2} = \frac{1}{2} \quad \text{for the cases } t = 2 \text{ and } 3.$$

In the later, we shall investigate these results more precisely.

Next, we shall consider the case $t = -1$. Since we defined $R_{(t\circ 1)}$ only for non-negative t, we shall modify the definition of the map $R_{(-1\circ 1)}$ as follows

$$R_{(-1\circ 1)} : \{1, \cdots, n-1\} \to \{1, \cdots, n^2-1\} \ , \ w \mapsto R_{(-1\circ 1)}(w) = (n-w)\circ w.$$

We call (x, y) has the $(-1\circ 1)$ *structure*, if

$$((n-x)\circ x)((n-y)\circ y) \equiv (n-z)\circ z \ mod\ n^2 \ \text{ for some } z \ (0 < z < n).$$

We have

$$((n-x)\circ x)((n-y)\circ y) \equiv xy(-2n+1) \equiv (a-2b)n + b \ mod\ n^2.$$

Combining this congruence relation and the condition $0 \le a, b < n$, we see that (x, y) has the $(-1\circ 1)$ structure if and only if

$$a - b \equiv 0 \ mod\ n \Longleftrightarrow a = b.$$

Therefore we have

$$K_{(-1\circ 1)}(n) = \#\{(x,y) | xy = a(n+1) \ (1 \le a < n)\}.$$

Put $d = (x, n+1)$. Then $1 < d < n+1$ and, for any d, x, y can be written $x = dx_0$ and $y = ((n+1)/d)y_0$ with unique x_0 and y_0, which satisfy

$$(x_0, (n+1)/d) = 1 \text{ and } \ 0 < y_0 < d.$$

Thus we have

$$\begin{aligned} K_{(-1\circ 1)}(n) &= \sum_{d|(n+1),\ 1<d<n+1} \left(\#\left\{x_0 \mid 1 \le x_0 < \frac{n+1}{d}, \left(x_0, \frac{n+1}{d}\right) = 1\right\}\right) \\ &\qquad \times (\#\{y_0 | 1 \le y_0 < d\}) \\ &= \sum_{d|(n+1)} \varphi\left(\frac{n+1}{d}\right)(d-1) - n \\ &= \sum_{d|(n+1)} \varphi\left(\frac{n+1}{d}\right)d - \sum_{d|(n+1)} \varphi\left(\frac{n+1}{d}\right) - n \\ &= (\varphi * i)(n+1) - 2n - 1. \end{aligned}$$

Here i is the arithmetic function such that $i(k) = k$ for any natural number k, and $*$ is the convolution of the arithmetic functions φ and i. Using the obvious relation $\varphi(x)y \le xy$, we can roughly estimate

$$\begin{aligned} K_{(-1\circ 1)}(n) &\le \sum_{d|(n+1)} \varphi(n+1) - 2n - 1 \\ &= d(n+1)\varphi(n+1) - 2n - 1 \\ &\le 2\sqrt{n+1}(n+1) - 2n - 1. \end{aligned}$$

Hence we can easily show the following theorem.

Theorem 6. *With the above notation, we have*

$$\limsup_{n\to\infty} \frac{\log(K_{(-1\circ 1)}(n))}{\log(n-1)^2} \leq \frac{3}{4}.$$

Next, we shall investigate the case $t = 0$. In the same way as above, we denote

$$K_{(0\circ 1)}(N) = \#\{(x,y) \mid (0 \circ x)(0 \circ y) \equiv (0 \circ z)\}.$$

Writing $xy = an + b$ with $0 \leq a, b < n$, we see (x,y) has the $(0 \circ 1)$ structure if and only if $a = 0$. Thus we see

$$\begin{aligned} K_{(0\circ 1)}(n) &= \#\{x | xy = b \ (1 \leq b < n)\} \\ &= \sum_{1 \leq b < n} d(b) \\ &= n \log n + (2\gamma - 1)n + O(\sqrt{n}). \end{aligned}$$

Here γ is the *Euler's constant* defined by

$$\gamma = \lim_{n\to\infty}(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n).$$

Therefore we have the following consequence:

Theorem 7.

$$\lim_{n\to\infty} \frac{\log K_{(0\circ 1)}(n)}{\log(n-1)^2} = \frac{1}{2}.$$

Remark 2. Let (n, e) be the public key system of Alice. Then Alice can divide the plain text into x with $x \leq \sqrt{n}$. Then Alice can define the redundancy function R of usual bit length by putting

$$R : x \mapsto 0 \circ x \ mod \ n.$$

Thus, substituting n to $\sqrt{n}$ in Theorem 7, we can estimate the security of this redundancy function R from the multiplicative attack.

Finally, we will study the redundancy function $K_{(2\circ 1)}(n)$ again. Write $xy = an + b$ with $0 < a, b < n$. Then we know that (x,y) has the $(2 \circ 1)$ structure if and only if $a + 2b = n$ or $2n$. In the following, we shall estimate $K_{(2\circ 1)}(n)$ as follows.

(I) Firstly, we shall treat the case $a + 2b = n$. Then we have

$$\begin{aligned}(2x)(2y) &= 4(an + b)\\ &= 4an + 2(n - a)\\ &= 2(2n - 1)a + (2n - 1) + 1\\ &\equiv 1 \ mod \ (2n - 1).\end{aligned}$$

We note that $0 < 2n - 1 - 2x$, $2n - 1 - 2y < 2n - 1$ and

$$(2n - 1 - 2x)(2n - 1 - 2y) \equiv 1 \ mod \ (2n - 1).$$

Since $2x$ is even and $2n - 1 - 2x$ is odd, we see the number of even numbers $0 < 2x < 2n - 1$ with $(2x, 2n - 1) = 1$ equals to the number of odd numbers $0 < 2y + 1 < 2n + 1$ with $(2y + 1, 2n + 1) = 1$. Thus the number of (x, y) with $(2x)(2y) \equiv 1 \ mod \ (2n - 1)$ satisfies

$$\#\{(x, y) \mid (2x)(2y) \equiv 1 \ mod \ (2n - 1)\} \leq \frac{\varphi(2n - 1)}{2}.$$

(II) Next, we shall treat the case $a + 2b = 2n$. Then we have

$$\begin{aligned}2xy &= 2(an + b)\\ &= 2an + (2n - a)\\ &= (2n - 1)a + (2n - 1) + 1\\ &\equiv 1 \ mod \ (2n - 1).\end{aligned}$$

Thus, in the same way as in (I), the number of the pairs (x, y) with $2xy \equiv 1 \ mod \ (2n - 1)$ satisfies

$$\#\{(x, y) \mid (2x)y \equiv 1 \ mod \ (2n - 1)\} \leq \frac{\varphi(2n - 1)}{2}.$$

Thus we have shown $K_{(2\circ 1)}(n) \leq \varphi(2n - 1)$ and proved the following theorem.

Theorem 8.

$$K_{(2\circ 1)}(n) \leq \varphi(2n - 1) \leq 2(n - 1) \ \textit{for any} \ n \geq 2.$$

Moreover, for any $0 < x < n$, we may expect the inverse of $2x$ *mod* $(2n - 1)$ distributes uniformly in the interval 0 and $2n - 1$. Thus we will give the following conjecture:

Conjecture.

$$\lim_{n\to\infty} \frac{K_{(2\circ 1)}(n)}{\varphi(2n-1)} = \frac{1}{2}.$$

Here we will give a table of the numbers $K_{(2\circ 1)}(n)$ $(n = 2^r)$ for small r which supports this conjecture.

$n = 2^r$	$\varphi(2n-1)$	$\varphi(2n-1)/2$	$K_{(2\circ 1)}(n)$
2	6	3	3
3	8	4	4
4	30	15	17
5	36	15	14
6	126	63	75
7	128	64	66
8	432	216	213
9	600	300	286
10	1936	968	999
11	1728	864	924
12	8190	4095	4093
13	10584	5292	5294
14	27000	13500	13699
15	32768	16384	16262
16	131070	65535	65661

Table 2: Calculations of $K_{(2\circ 1)}(2^r)$ using UBASIC86

Remark 3. In [8], we have shown that $K_{(3\circ 1)}(n)$ satisfies the analogous results as above and formulated similar conjecture for any odd n.

4. Numerical data

In the following, we shall give the numerical data to generate and verify the signature with the redundancy function R_2. We used a text m of the bit length 7.39KB and used the *Timing* of Mathematica 4.1. In the following "Normal" is the time(second) which took to generate and verify the signature s of the text m. "Redundancy" is the time(second) which took to generate and verify the signature of the text $m_1 = R_2(m)$. Let (n, e) be the RSA signature system with $ed \equiv 1 \ mod \ \varphi(n^2)$. Then We know the complexity to sign the normal text m is $O((\log n)^2 \cdot \log d)$, while the complexity to sign the text with R_2 is $O((\log(n^2))^2 \cdot \log d)$. Thus we can expect the time to generate and verify the signature with the redundancy function R_2 takes about $4 \sim 8$ times as the usual one. In practice, it took about $2 \sim 3$ times as follows.

The bit length of p and q	Generation		Verification	
	Normal	Redundancy	Normal	Redundancy
106	0.312(sec.)	0.516	0.313(sec.)	0.469
212	0.531	1.219	0.562	1.266
318	0.781	2.172	0.781	2.156
425	1.156	3.359	1.172	3.328

Table 3: Practical time to generate and verify, using Mathematica 4.1

References

[1] J. A. Buchmann, Introduction to Cryptography, Springer–Verlag, New York, 2001.

[2] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 5th ed., Oxford University Press, Oxford, 1979.

[3] H. Hatalová and T. Šalát, Remarks on two results in the elementary theory of numbers, *Acta Fac. Rer. Natur. Univ. Comenian. Math.* **20** (1969), 113-117.

[4] Y. Kida, User's Manual for UBASIC86 [8.7], Nihon-hyoronsha, Tokyo, 1994.

[5] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, New York, 1997.

[6] D. S. Mitrinović, J. Săndor and B. Cristici, Handbook of Number Theory, Kluwer Academic Publishers, Dordrecht, 1996.

[7] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, **21**, (1978), 120-126.

[8] H. Yasui, On RSA signatures with redundancy, Master Thesis (2004) Tokushima University (in Japanese).

J. Math. Univ. Tokushima
Vol.39 (2005), 23-46

A Geometrical Formulation for Classical Mechanics in Gauge Fields*

By

Ruishi Kuwabara

Faculty of Integrated Arts and Sciences,
The University of Tokushima,
Minami-Josanjima, Tokushima 770-8502, JAPAN
e-mail: kuwabara@ias.tokushima-u.ac.jp

(Received September 30, 2005)

Abstract

We give a geometrical formulation for the classical mechanics in a non-abelian gauge field on a Riemannian manifold. The formulation is based on the reduction procedure associated to the non-abelian symmetry in the principal bundle which describes the gauge field. In the formulation we present explicitly the equation of the motion (called Wong's equation) of a charged particle by using a local coordinate system.

2000 Mathematics Subject Classification. 53D20

Introduction

Let (M, m) be an n dimensional smooth Riemannian manifold without boundary, and let $\pi : P \to M$ be a principal G-bundle, where G is a compact Lie group with $\mathfrak{g}$ its Lie algebra. Suppose P is endowed with a connection $\widetilde{\nabla}$. Take an open covering $\{U_\alpha\}$ of M with $\{\varphi_{\alpha\beta}\}$ being the transition functions of P. Then the curvature of $\widetilde{\nabla}$ is regarded as a family of $\mathfrak{g}$-valued two forms $\bar{\Theta}_\alpha$ defined on U_α which satisfies

$$\bar{\Theta}_\beta = \mathrm{Ad}(\varphi_{\alpha\beta}^{-1})\bar{\Theta}_\alpha \tag{0.1}$$

on $U_\alpha \cap U_\beta (\neq \phi)$, where $\mathrm{Ad}(\cdot)$ denotes the adjoint action of G on $\mathfrak{g}$. Such a family of $\mathfrak{g}$-valued two forms $\{\bar{\Theta}_\alpha\}$ on M satisfying (0.1) is called a *gauge field*. When G is the abelian group $U(1)$, $\bar{\Theta}_\alpha = \bar{\Theta}_\beta$ holds, and accordingly we have a two-form $\bar{\Theta}$ globally defined on M, which is called a *magnetic field*.

In the previous papers [10], [11], [12] we have considered the case where $G = U(1)$, namely the classical and the quantum mechanics in magnetic fields, and clarified some relations between the classical orbits and the energy levels of the Schrödinger operator. In those papers the geometrical formulation for the magnetic dynamical system based on the reduction procedure associated

*This research is partially supported by Grant-in-Aid for Scientific Research (C) (No.14540210) of JSPS.

to the $U(1)$-symmetry of the system plays key role in the investigations. In the present article we generalize the formulation for the magnetic systems to the case of a non-abelian compact Lie group G, which describe the motion of a (classical) particle in a non-abelian gauge field.

Various mathematical formulations of the equation of classical motion of a particle in the (non-abelian) gauge field (or the Yang-Mills field) have been presented by Kerner [5], Guillemin-Sternberg [3], [4], Kummer [9] and so on. (See also Montgomery [14].) We give in this article a slightly different formulation based on the reduction procedure for the symplectic G-action on the cotangent bundle T^*P, and present the equation of the motion (called Wong's equation) explicitly by using a local coordinate system.

The organization of the article is as follows. In §1 we introduce the so-called Kaluza-Klein metric on P associated to the connection $\widetilde{\nabla}$, and the metrics on M and G. Thus we get the Hamiltonian system $(T^*P, \Omega_P, \widetilde{H})$ of geodesic flow on T^*P. Then in §2 because of the G-invariance the system $(T^*P, \Omega_P, \widetilde{H})$ is reduced to $(P_\mu, \Omega_\mu, H_\mu)$ according to the Marsden-Weinstein reduction procedure (see [13], [1]). We clarify in §3 the reduced phase space P_μ is the fiber bundle over T^*M with the fiber being a co-adjoint orbit through μ in $\mathfrak{g}^*$. In §4 we show that the reduced system $(P_\mu, \Omega_\mu, H_\mu)$ is realized as the subsystem of $(T^*M_\mu, \widetilde{\Omega}_\mu, \widetilde{H}_\mu)$, where the manifold M_μ is a union of the spaces of (external) configurations and of internal degrees of freedom, and the symplectic structure $\widetilde{\Omega}_\mu$ is derived explicitly from the connection form (or the gauge potential) of $\widetilde{\nabla}$. Section 5 gives a explicit expression of the flow or the equation of motion (called Wong's equation) in the system $(T^*M_\mu, \widetilde{\Omega}_\mu, \widetilde{H}_\mu)$ by using local coordinates. Finally in §6 we consider the Hopf bundle over the quaternionic projective space, which is a typical example in non-abelian gauge theory.

1 Kaluza-Klein metric on the principal bundle

Let $\pi : P \to M$ be a principal G-bundle over an n-dimensional Riemannian manifold (M, m) without boundary, where G is an r-dimensional compact Lie group. Suppose P is endowed with a connection $\widetilde{\nabla}$, i.e., the direct decomposition of each tangent space T_uP $(u \in P)$ as

$$T_uP = H_u \oplus V_u, \tag{1.1}$$

where V_u is tangent to the fiber, and H_u is linearly isomorphic with $T_{\pi(u)}M$ through $\pi_*|_{H_u}$ and satisfies

$$H_{u \cdot g} = R_{g*}(H_u) \tag{1.2}$$

for the right action R_g of $g \in G$ on P (cf. [8]). Note that the tangent space V_u to the fiber is linearly isomorphic with $\mathfrak{g}$ by the correspondence $\mathfrak{g} \ni A \mapsto$

$A_u^P := \frac{d}{dt}(u \cdot \exp tA)|_{t=0} \in V_u$. Let us take an inner product $(\,,\,)_{\mathfrak{g}}$ on $\mathfrak{g} \cong T_eG$ (e : the identity of G) which is invariant under the adjoint action of G (such inner product induces a right- and left-invariant metric on G). Then, $(,)_{\mathfrak{g}}$ induces the inner product $(\,,\,)_{V,u}$ on V_u ($u \in P$) as $(A^P, B^P)_{V,u} = (A,B)_{\mathfrak{g}}$ ($A, B \in \mathfrak{g}$). On the other hand, we have the inner product $(\,,\,)_{H,u}$ on H_u from the metric m on M such that $\pi_*|_{H_u}$ is an isometry. Finally, we define an inner product $\widetilde{m}$ in each T_uP ($u \in P$) by defining H_u and V_u to be orthogonal each other. The metric $\widetilde{m}$ on P (which is induced from the metric m on M, the Ad-invariant metric on $\mathfrak{g}$, and the connection (1.1)) is called the *Kaluza-Klein metric* (cf. [5]). Note that $\widetilde{m}$ is invariant under the G-action on P because of the Ad-invariance of the metric of $\mathfrak{g}$ and the property (1.2).

Let $\Omega_P = d\omega_P$ be the standard symplectic structure on the cotangent bundleT^*P of P, where ω_P is called the canonical one form on T^*P. We have the natural Hamiltonian function $\widetilde{H}$ on T^*P defined by the Kaluza-Klein metric $\widetilde{m}$. Thus, we have the Hamiltonian system $(T^*P, \Omega_P, \widetilde{H})$, which is just the system of geodesic flow on T^*P generated by the Hamiltonian vector field $X_{\widetilde{H}}$ induced from $\widetilde{H}$, i.e., $i(X_{\widetilde{H}})\Omega_P = -d\widetilde{H}$, where $i(X_{\widetilde{H}})\Omega_P$ stands for the interior product of $X_{\widetilde{H}}$ and Ω_P.

2 The momentum map and the reduction of the system

The action $p \mapsto p \cdot g = R_g(p)$ ($p \in P$, $g \in G$) of G on P is naturally lifted to the action $R^*_{g^{-1}} := (R_{g^{-1}})^*$ on T^*P (so that $R^*_{g^{-1}} : T^*_pP \to T^*_{p\cdot g}P$ for each $p \in P$), and the action $R^*_{g^{-1}}$ preserves ω_P (and accordingly Ω_P), i.e., $R^*_{g^{-1}}\omega_P = \omega_P$ holds for every $g \in G$. (We call such action a *symplectic action.*) Moreover, we notice that the Hamiltonian $\widetilde{H}$ is also invariant under the action $R^*_{g^{-1}}$.

A momentum map for the symplectic G-action is a map $J : T^*P \to \mathfrak{g}^*$ satisfying

$$\langle J(p), A\rangle = \langle p_u, A_u^P\rangle = i(A_p^{T^*P})\omega_P \quad (p \in T^*P,\ p_u \in T_u^*P\ (u \in P)), \tag{2.1}$$

for all $A \in \mathfrak{g}$, where $A_p^{T^*P} := \frac{d}{dt}(R^*_{g(t)^{-1}}(p))\big|_{t=0}$ with $g(t) = \exp tA$.

Lemma 2.1 *(1) The momentum map J is surjective onto $\mathfrak{g}^*$, and every $\mu \in \mathfrak{g}^*$ is a regular value of J.*

(2) The momentum map J is Ad**-equivariant, i.e.,*

$$J \circ R^*_{g^{-1}} = \mathrm{Ad}^*(g^{-1}) \circ J \tag{2.2}$$

holds for $g \in G$. Here we define $\mathrm{Ad}^*(g) := (\mathrm{Ad}(g^{-1}))^*$ *(the adjoint of* $\mathrm{Ad}(g^{-1}) : \mathfrak{g} \to \mathfrak{g}$*).*

(3) The momentum map J is invariant under the geodesic flow on T^*P, i.e., $X_{\widetilde{H}}J = 0$ holds.

Proof. (1) Note the definition (2.1) of J, we can easily derive the assertion from the fact that the map $\mathfrak{g} \ni A \mapsto A_u^P \in T_uP$ is surjective.

(2) For $p \in T_u^*P$, $A \in \mathfrak{g}$ we have

$$\langle J(R_{g^{-1}}^*(p)), A\rangle = \langle R_{g^{-1}}^*(p_u), A_{u\cdot g}^P\rangle = \langle p_u, R_{g^{-1}*}(A_{u\cdot g}^P)\rangle.$$

Since

$$\begin{aligned} R_{g^{-1}*}(A_{u\cdot g}^P) &= \frac{d}{dt}(u \cdot g\exp(tA)g^{-1})|_{t=0} \\ &= \frac{d}{dt}(u \cdot \exp(t\mathrm{Ad}(g)A))|_{t=0} = [\mathrm{Ad}(g)A]_u^P, \end{aligned}$$

we have

$$\langle J(R_{g^{-1}}^*(p)), A\rangle = \langle p_u, [\mathrm{Ad}(g)A]_u^P\rangle = \langle J(p), \mathrm{Ad}(g)A\rangle = \langle \mathrm{Ad}^*(g^{-1})J(p), A\rangle.$$

(3) For $A \in \mathfrak{g}$ define the function J_A on T^*P as $J_A(p) = \langle J(p), A\rangle = i(A^{T^*P})\omega_P$. We show $X_{\widetilde{H}}J_A = 0$. First note that the Lie derivative $\mathcal{L}_{A^{T^*P}}\omega_P = d(i(A^{T^*P})\omega_P) + i(A^{T^*P})d\omega_P = 0$ because G-action on T^*P preserves ω_P. We have

$$\begin{aligned} X_{\widetilde{H}}J_A &= X_{\widetilde{H}}(i(A^{T^*P})\omega_P) = \langle d(i(A^{T^*P})\omega_P), X_{\widetilde{H}}\rangle \\ &= -\langle i(A^{T^*P})d\omega_P, X_{\widetilde{H}}\rangle = \langle i(X_{\widetilde{H}})d\omega_P, A^{T^*P}\rangle \\ &= -\langle d\widetilde{H}, A^{T^*P}\rangle = 0. \end{aligned}$$

Here note that G-action also preserves $\widetilde{H}$. □

Now, we apply the reduction procedure associated to the momentum map J by Marsden and Weinstein. For $\mu \in \mathfrak{g}^*$, it follows from Lemma 2.1 that $J^{-1}(\mu)$ is a $(2n+r)$-dimensional submanifold of T^*P, which is invariant under the geodesic flow. Let $G_\mu := \{g \in G | \mathrm{Ad}^*(g)\mu = \mu\} \subset G$, which is a closed subgroup of G. Then, by virtue of Lemma 2.1,(2) G_μ preserves the submanifold $J^{-1}(\mu)$, and the action of G_μ on $J^{-1}(\mu)$ is free. Hence the quotient set $P_\mu := J^{-1}(\mu)/G_\mu$ is a smooth manifold, and the natural projection

$$\pi_\mu : J^{-1}(\mu) \to P_\mu$$

is a submersion. In this situation we have the following.

Proposition 2.2 *The quotient manifold P_μ has a uniquely defined symplectic form Ω_μ with*

$$\pi_\mu^*\Omega_\mu = i_\mu^*\Omega_P,$$

where $i_\mu : J^{-1}(\mu) \hookrightarrow T^*P$ is the inclusion.

Sketch of the proof. Note that the following facts: For $p \in T^*P$,

(i) $T_p(J^{-1}(\mu)) = \mathrm{Ker}(J_*) \cong \{X \in T_p(T^*P) | \, \Omega_P(X, A_p^{T^*P}) = 0 \text{ for } \forall A \in \mathfrak{g}\}$, and

(ii) $T_p(J^{-1}(\mu))/T_p(G_\mu \cdot p) \cong T_{\pi_\mu(p)}(P_\mu)$.

For $X \in T_p(J^{-1}(\mu))$, let $[X] = \pi_{\mu *}(X)$ be the associated equivalence class in $T_p(J^{-1}(\mu))/T_p(G_\mu \cdot p)$. Let us define Ω_μ on P_μ as

$$\Omega_\mu([X],[Y]) := \Omega_P(X,Y) \qquad (\, X, Y \in T_p(J^{-1}(\mu))\,).$$

Here we can easily check that Ω_μ is well-defined by the above fact (i) and that Ω_P is invariant under the G_μ-action. Moreover, we can check that Ω_μ is closed and non-degenerate. These properties are guaranteed by those of Ω_P. □

The Hamiltonian $\widetilde{H}$ is G_μ-invariant, and accordingly induces the (Hamiltonian) function H_μ on P_μ. Thus, we have a reduced Hamiltonian system $(P_\mu, \Omega_\mu, H_\mu)$, where $\dim P_\mu = 2n + r - r_\mu$ ($r_\mu := \dim G_\mu$).

Let $\mathcal{O}_\mu$ be the coadjoint orbit of μ in $\mathfrak{g}^*$, i.e.,

$$\mathcal{O}_\mu := \{\mathrm{Ad}^*(g)\mu \mid g \in G\},$$

which is diffeomorphic with G/G_μ. Then, we have the following.

Proposition 2.3 *Suppose ν is an element of $\mathcal{O}_\mu$. Then, the reduced Hamiltonian system $(P_\nu, \Omega_\nu, H_\nu)$ associated to $\nu \in \mathfrak{g}^*$ is isomorphic with $(P_\mu, \Omega_\mu, H_\mu)$.*

Proof. Suppose $\nu = \mathrm{Ad}^*(g)\mu$ for $g \in G$. Note that $G_\mu \cong G_\nu$ by the isomorphism $G_\mu \ni h \mapsto ghg^{-1} \in G_\nu$. By virtue of Lemma 2.1,(2), we have the map $R_g^* : J^{-1}(\mu) \to J^{-1}(\nu)$. Then, we can easily see that R_g^* induces the isomorphism of $(P_\mu, \Omega_\mu, H_\mu)$ onto $(P_\nu, \Omega_\nu, H_\nu)$. □

3 Geometrical structure of the reduced space

We can define the surjective map $\Phi : T^*P \to T^*M$ associated to the connection $\widetilde{\nabla}$ on P as follows. Let p be a point in T^*P with $\pi_P(p) = u \in P$, $\pi(u) = x \in M$, where $\pi_P : T^*P \to P$ is a natural projection. For a tangent vector $X \in T_xM$, let $X_u^\#$ be the horizontal lift of X relative to the connection $\widetilde{\nabla}$, i.e., $X^\#$ belongs to H_u in (1.1) and $\pi_*(X_u^\#) = X$. We define $\Phi(p) \in T_x^*M$ as

$$\langle \Phi(p), X \rangle := \langle p, X_u^\# \rangle \qquad (X \in T_xM).$$

Concerning the horizontal lifts we have $X_{u \cdot g}^\# = R_{g*}(X_u^\#)$, and accordingly see that Φ is G-invariant, i.e., $\Phi(R_{g^{-1}}^*(p)) = \Phi(p)$ as follows:

$$\langle \Phi(R_{g^{-1}}^*(p)), X \rangle = \langle R_{g^{-1}}^*(p), X_{u \cdot g}^\# \rangle = \langle p, X_u^\# \rangle = \langle \Phi(p), X \rangle.$$

By virtue of the G-invariance (hence, the G_μ-invariance) of Φ we have the surjective map $\Phi_\mu : P_\mu \to T^*M$ induced from Φ. The purpose of this subsection is to show the following.

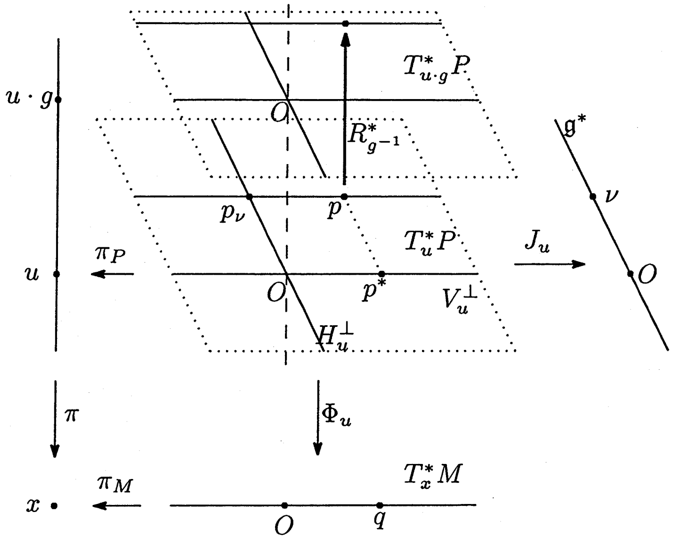

Figure 1: Reduced space

Proposition 3.1 *$\Phi_\mu : P_\mu \to T^*M$ is a fiber space with the fiber being the coadjoint orbit $\mathcal{O}_\mu$ of μ in $\mathfrak{g}^*$.*

We have the decomposition of T^*_uP associated to (1.1):

$$T^*_uP = H_u^\perp \oplus V_u^\perp,$$

where

$$\begin{aligned} H_u^\perp &:= \{p \in T^*_uP |\ \langle p, X \rangle = 0 \text{ for } \forall X \in H_u\}, \\ V_u^\perp &:= \{p \in T^*_uP |\ \langle p, A^P \rangle = 0 \text{ for } \forall A^P \in V_u\}. \end{aligned}$$

Note that $\dim H_u^\perp = r$ and $\dim V_u^\perp = n$. The following lemma is easily obtained.

Lemma 3.2 *(1) The map $J_u := J|_{H_u^\perp} : H_u^\perp \to \mathfrak{g}^*$ is a linear isomorphism.*

(2) For $\nu \in \mathfrak{g}^*$ let $p_\nu = J_u^{-1}(\nu) \in H_u^\perp$. Then,

$$J^{-1}(\nu) \cap T^*_uP = p_\nu + V_u^\perp := \{p_\nu + p^* \mid p^* \in V_u^\perp\}.$$

(3) The map $\Phi_{u,\nu} := \Phi|_{p_\nu + V_u^\perp} : J^{-1}(\nu) \cap T^*_uP \to T^*_xM$ is a bijection with $\Phi_{u,\nu}(p_\nu) = 0$.

Proof. (1)It is obvious that J_u is linear and surjective. Suppose $J(p) = J(p')$ for $p,\ p' \in H_u^{\perp}$. Then, $\langle p, A_u^P \rangle = \langle p', A_u^P \rangle$ for $\forall A \in \mathfrak{g}$. On the other hand, $\langle p, X \rangle = \langle p', X \rangle = 0$ for $\forall X \in H_u$. Hence, $\langle p, V \rangle = \langle p', V \rangle$ for $\forall V \in T_uP$, and accordingly $p = p'$

(2) is obvious.

(3) The surjectivity is obvious. Suppose $\Phi(p) = \Phi(p')$ for $p,\ p' \in J^{-1}(\nu) \cap T_u^*P$. Then, $\langle p, X_u^{\#} \rangle = \langle p', X_u^{\#} \rangle$ for $\forall X \in T_xM$. On the other hand, $\langle p, A_u^P \rangle = \langle p', A_u^P \rangle = \langle \nu, A \rangle$ for $\forall A \in \mathfrak{g}$. Hence, $\langle p, V \rangle = \langle p', V \rangle$ for $\forall V \in T_uP$, and accordingly $p = p'$ □

Let u be a point in P with $\pi(u) = x \in M$. We define the map ψ_u of $T_x^*M \times \mathcal{O}_\mu$ to $J^{-1}(\mu)$ as

$$T_x^*M \times \mathcal{O}_\mu \ni (q, \nu) \mapsto R_{g^{-1}}^*(\Phi_{u,0}^{-1}(q) + J_u^{-1}(\nu)) \in T_{u \cdot g}^*P \cap J^{-1}(\mu),$$

where g is an element of G satisfying $\nu = \mathrm{Ad}^*(g)\mu$. Here we can check by noticing (2.2) and $\Phi_{u,0}^{-1}(q) \in V_u^{\perp}$ that the image of Ψ_u belongs to $J^{-1}(\mu)$ as follows:

$$J(R_{g^{-1}}^*(\Phi_{u,0}^{-1}(q) + J_u^{-1}(\nu))) = J(R_{g^{-1}}^*(J_u^{-1}(\nu))) = \mathrm{Ad}^*(g^{-1})\nu = \mu.$$

If $\nu = \mathrm{Ad}^*(g)\mu = \mathrm{Ad}^*(g')\mu$ for $g \neq g'$, then $g' = gh$ for some $h \in G_\mu$. Therefore, we obtain the bijective map

$$\Psi_u : T_x^*M \times \mathcal{O}_\mu \to \Big[\big(\bigcup_{g \in G} T_{u \cdot g}^*P\big) \cap J^{-1}(\mu)\Big] \Big/ G_\mu$$

from ψ_u. It is easily see that Ψ_u is bijective and satisfies $\Phi_\mu \circ \Psi_u(q, \nu) = q$. Thus it is shown that $\Phi_\mu : P_\mu \to T^*M$ is a fiber space with the fiber being the coadjoint orbit $\mathcal{O}_\mu$. Moreover, by taking a local section $u = u(x)$ $(x \in U \subset M)$ of P we have a local triviality of P_μ:

$$\Psi_u : T^*U \times \mathcal{O}_\mu \overset{\cong}{\longrightarrow} \Phi_\mu^{-1}(T^*U).$$

In particular, we have a local section $s(q)$ $(q \in T^*U)$ of the fiber space $\Phi_\mu : P_\mu \to T^*M$ by

$$s_u(q) := \Psi_u(q, \mu) = [\Phi_{u,0}^{-1}(q) + J_u^{-1}(\mu)]. \tag{3.1}$$

associated to a local section $u(x)$ $(x \in U)$ of P. Thus we complete the proof of Proposition 3.1. □

4 Dynamical structure of the reduced system

Let θ be the connection form on P of the connection $\widetilde{\nabla}$. The connection form θ is a $\mathfrak{g}$-valued one form satisfying (i) $\theta(A^P) = A$ for $\forall A \in \mathfrak{g}$, and (ii)

$R_g^*\theta = \mathrm{Ad}(g^{-1})\theta$ for $\forall g \in G$. For $\mu \in \mathfrak{g}^*$ we define the $\mathbb{R}$-valued one form θ_μ on P by

$$\theta_\mu(X) := \langle \mu, \theta(X) \rangle \qquad (X \in T_uP).$$

It is easy to see that θ_μ is G_μ-invariant, i.e., $R_g^*\theta_\mu = \theta_\mu$ for $\forall g \in G_\mu$. Let $\mathfrak{g}_\mu$ be the Lie algebra of G_μ. Then we have

Lemma 4.1 *$d\theta_\mu(A^P, X) = 0$ holds for any $A \in \mathfrak{g}_\mu$ and $X \in T_uP$.*

Proof. We have

$$d\theta_\mu(A^P, X) = (i(A^P)d\theta_\mu)(X) = (\mathcal{L}_{A^P}\theta_\mu)(X) - d(i(A^P)\theta_\mu)(X) = 0$$

because θ_μ is G_μ-invariant and $i(A^P)\theta_\mu = \theta_\mu(A^P) = \langle \mu, A \rangle =$ constant. □

Let $M_\mu := P/G_\mu$ be the quotient manifold by the G_μ-action on P. By noticing the above lemma the two form $d\theta_\mu$ can be regarded as that on M_μ as

$$d\theta_\mu([X],[Y]) := d\theta_\mu(X, Y) \qquad (X, Y \in T_uP).$$

Now, we consider the cotangent bundle T^*M_μ with the twisted symplectic form

$$\widetilde{\Omega}_\mu := \Omega_{M_\mu} + \pi_{M_\mu}^*(d\theta_\mu), \tag{4.1}$$

where Ω_{M_μ} is the canonical symplectic two form on T^*M_μ and $\pi_{M_\mu} : T^*M_\mu \to M_\mu$ is the projection.

Proposition 4.2 *([1, Theorem 4.3.3], [9, Theorem 3]) There exists a symplectic embedding*

$$\chi_\mu : (P_\mu, \Omega_\mu) \hookrightarrow (T^*M_\mu, \widetilde{\Omega}_\mu),$$

that is, χ_μ is an embedding satisfying $\chi_\mu^*\widetilde{\Omega}_\mu = \Omega_\mu$.

Proof. For each $u \in P$ let

$$(V_\mu)_u^\perp := \{p \in T_u^*P \mid \langle p, A_u^P \rangle = 0 \text{ for } \forall A \in \mathfrak{g}_\mu\} \ (\subset T_u^*P),$$

which can be identified with $T_q^*M_\mu$ ($q = \pi'(u) \in M_\mu$ for the projection $\pi' : P \to M_\mu$) because we have the linear isomorphism

$$R_{g^{-1}}^* : (V_\mu)_u^\perp \to (V_\mu)_{u\cdot g}^\perp$$

for each $g \in G_\mu$. Thus we have $T^*M_\mu \cong V_\mu^\perp/G_\mu$.

Take $p \in T^*P$ such that $\pi_P(p) = u \in P$, i.e., $p \in T_u^*P$. We define $\bar{\chi}_\mu(p) = p_u - (\theta_\mu)_u \in T_u^*P$. Then we can easily see that (i) $\bar{\chi}_\mu(p)$ belongs to $V_u^\perp$ (and accordingly to $(V_\mu)_u^\perp$) if $p_\mu \in J^{-1}(\mu)$, and (ii) $\bar{\chi}_\mu(R_{g^{-1}}^*(p)) = R_{g^{-1}}^*(\bar{\chi}_\mu(p))$ for $g \in G_\mu$, i.e., $\bar{\chi}_\mu$ is G_μ-equivariant. In fact, (i) is shown as $\langle p_u, A_u^P \rangle - \langle (\theta_\mu)_u, A_u^P \rangle = \langle J(p), A \rangle - \langle \mu, A \rangle = 0$. As (ii) we have only to see the equality

$(\theta_\mu)_{u\cdot g} = R^*_{g^{-1}}((\theta_\mu)_u)$, that is shown as $(\theta_\mu)_{u\cdot g}(X) = R^*_{g^{-1}}((\theta_\mu)_u)(X) = 0$ for $\forall X \in H_{u\cdot g}$ and $(\theta_\mu)_{u\cdot g}(A^P_{u\cdot g}) = R^*_{g^{-1}}((\theta_\mu)_u)(A^P_{u\cdot g}) = \langle \mu, A\rangle$ for $\forall A \in \mathfrak{g}$. As a result of (i) and (ii) $\bar{\chi}_\mu$ induces the map $\chi_\mu : P_\mu(= J^{-1}(\mu)/G_\mu) \to T^*M_\mu(= V_\mu^\perp/G_\mu)$. It is obvious that χ_μ is an injection.

Now, we will show that $\chi_\mu^*\widetilde{\Omega}_\mu = \Omega_\mu$. Let X be a vector in $T_p(T^*P)$ $(p \in T^*P, \pi_P(p) = u)$. Then, X is expressed as

$$X = \bar{X} + X^* \quad \text{with } \bar{X} \in T_uP,\ X^* \in T^*_uP(= T_p(T^*_uP)).$$

Here X^* belongs to $V_u^\perp$ if $X \in T_pJ^{-1}(\mu)$ (Lemma 3.2,(2)). For two vector fields $X = X(p)$, $Y = Y(p)$ on a neighborhood of p_0 in $J^{-1}(\mu)$ we have

$$\begin{aligned}\Omega_P(X,Y) &= \frac{1}{2}\{X\langle\omega_P, Y\rangle - Y\langle\omega_P, X\rangle - \langle\omega_P, [X,Y]\rangle\}\\ &= \frac{1}{2}\{X\langle p, \bar{Y}\rangle - Y\langle p, \bar{X}\rangle - \langle p, \overline{[X,Y]}\rangle\}.\end{aligned}$$

Put $p'(= \bar{\chi}_\mu(p)) = p - \theta_\mu$, and we have

$$\begin{aligned}\Omega_P(X,Y) &= \frac{1}{2}\{X\langle p', \bar{Y}\rangle - Y\langle p', \bar{X}\rangle - \langle p', \overline{[X,Y]}\rangle\}\\ &+ \frac{1}{2}\{\bar{X}\langle\theta_\mu, \bar{Y}\rangle - \bar{Y}\langle\theta_\mu, \bar{X}\rangle - \langle\theta_\mu, \overline{[X,Y]}\rangle\}.\end{aligned}$$

Noticing $V_u^\perp \subset (V_\mu)_u^\perp$ we can regard $X = \bar{X} + X^*$ as a vector in $T_{p'}(T^*M_\mu)$, and see that the first term is nothing but $\Omega_{M_\mu}(\chi_{\mu*}([X]), \chi_{\mu*}([Y]))$. By noticing $\overline{[X,Y]} = [\bar{X}, \bar{Y}]$ we see that the second term is just
$d\theta_\mu((\pi_{M_\mu}\circ\chi_\mu)_*([X]), (\pi_{M_\mu}\circ\chi_\mu)_*([Y]))$. □

Next, we define the Riemannian metric m_μ on M_μ as follows. Put $(V_\mu)_u := T_u(G_\mu \cdot u)$ for $u \in P$, which is a subspace of V_u. Then we have the orthogonal decomposition

$$T_uP = H_u \oplus V_u = H_u \oplus (H_\mu)_u \oplus (V_\mu)_u \tag{4.2}$$

from (1.1) and the G-invariant metric on G, where $(H_\mu)_u$ is the orthogonal compliment of $(V_\mu)_u$ in V_u. By identifying T_uM_μ with $H_u \oplus (H_\mu)_u$ we obtain the metric m_μ on T_uM_μ.

Let $\widetilde{H}_\mu$ be the Hamiltonian function on T^*M_μ naturally induced from the metric m_μ. Then,

Lemma 4.3 *$H_\mu = \chi_\mu^*\widetilde{H}_\mu + \|\mu\|^2_{\mathfrak{g}^*}$, where $\|\cdot\|_{\mathfrak{g}^*}$ is the naturally induced norm from the inner product in* $\mathfrak{g}$.

Proof. For $p \in T^*_uP \cap J^{-1}(\mu)$ we have $p = \bar{\chi}_\mu(p) + (\theta_\mu)_u$ with $\bar{\chi}_\mu(p) \in V_u^\perp$ and $(\theta_\mu)_u \in H_u^\perp$. Since $V_u^\perp$ and $H_u^\perp$ are orthogonal each other, we have

$$H_\mu([p]) = \|\bar{\chi}_\mu(p)\|^2 + \|(\theta_\mu)_u\|^2 = \widetilde{H}_\mu(\chi_\mu([p])) + \|(\theta_\mu)_u\|^2.$$

$$\begin{tikzcd}
& & & T^*P \arrow[r, "J"] \arrow[llld, "\pi_P"'] & \mathfrak{g}^* \\
P \arrow[dd, "\pi"'] \arrow[dr] & & & J^{-1}(\mu) \arrow[u, "\text{incl.}"'] \arrow[d, "\pi_\mu"] & \\
& M_\mu \arrow[dl] & T^*M_\mu \arrow[l, "\pi_{M_\mu}"'] & P_\mu(= J^{-1}(\mu)/G_\mu) \arrow[l, hook', "\chi_\mu"'] \arrow[d, "\Phi_\mu"] & \\
M & & & T^*M \arrow[lll, "\pi_M"'] &
\end{tikzcd}$$

Figure 2: Reduction procedure

Note that $(\theta_\mu)_u(A_u^P) = \langle \mu, A \rangle$ for $\forall A \in \mathfrak{g}$, and we have $\|(\theta_\mu)_u\| = \|\mu\|_{\mathfrak{g}^*}$. □

As a consequence, we have the following (cf. Figure 2).

Proposition 4.4 *The reduced Hamiltonian system $(P_\mu, \Omega_\mu, H_\mu)$ is regarded as a Hamiltonian subsystem of $(T^*M_\mu, \widetilde{\Omega}_\mu, \widetilde{H}_\mu)$.*

Let X_μ be the Hamiltonian vector field on P_μ associated to H_μ, that is, $i(X_\mu)\Omega_\mu = -dH_\mu$. The flow of X_μ is regarded as embedded Hamiltonian flow in $(T^*M_\mu, \widetilde{\Omega}_\mu, \widetilde{H}_\mu)$, and represents the motion of a classical particle of "charge" μ in the gauge field given by the connection $\widetilde{\nabla}$. The (external) configuration space of the system is the manifold M and the fiber of $M_\mu \to M$ is the space of internal degrees of freedom.

5 Expressions in local coordinate systems

5.1 Basic formulas

Let $\{Y_\alpha\} = \{Y'_\alpha, Y''_\beta\} = \{Y'_1, \ldots, Y'_{r_1}, Y''_{r_1+1}, \ldots, Y''_r\}$ be the orthonormal basis of $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{g}_\mu$ with $\{Y'_\alpha\}$, $\{Y''_\beta\}$ being the basis of $\mathfrak{m}$ and $\mathfrak{g}_\mu$, respectively, where $\mathfrak{g}_\mu$ is the Lie algebra of G_μ. Note that $\dim G_\mu = r - r_1 (= r_\mu)$. We have coordinates $y = (y', y'') = (y'^1, \ldots, y'^{r_1}, y''^{r_1+1}, \ldots, y''^r)$ in a neighborhood V of the identity $(y = 0)$ of G by

$$\begin{aligned} y &= (y'^1, \ldots, y'^{r_1}, y''^{r_1+1}, \ldots, y''^r) \\ &\longleftrightarrow\; g = \exp\Big(\sum_{\alpha=1}^{r_1} y'^\alpha Y'_\alpha\Big) \exp\Big(\sum_{\beta=r_1+1}^{r} y''^\beta Y''_\beta\Big). \end{aligned}$$

By virtue of the local triviality of the bundle P we take a local coordinate $(x^i, y^\alpha) \in U \times V$ ($U \subset M$, $V \subset G$) of P. For the basis $\{Y_\alpha\}$ of $\mathfrak{g}$ we have the associated basis $\{Y_\alpha^P\}$ of V_u, which is expressed as

$$Y_\alpha^P(x,y) = \sum_{\beta=1}^{r} \Gamma_\alpha^\beta(y) \frac{\partial}{\partial y^\beta} \tag{5.1}$$

with $\Gamma_\alpha^\beta(0) = \delta_\alpha^\beta$. Let $(x^i, y^\alpha; \xi_i, \eta_\alpha)$ the local canonical coordinates of T^*P. Then, the momentum map J is represented as

$$J(x,y;\xi,\eta) = \sum_{\alpha=1}^{r} \Big(\sum_{\beta=1}^{r} \Gamma_\alpha^\beta(y)\eta_\beta \Big) Y^\alpha \in \mathfrak{g}^*, \tag{5.2}$$

where $\{Y^1, \dots, Y^r\}$ is the dual basis of $\mathfrak{g}^*$ associated to $\{Y_\alpha\}$.

We remark that $\Gamma(y) := (\Gamma_\alpha^\beta(y))$ in (5.1) is non-singular near $y = 0$ because $\Gamma_\alpha^\beta(0) = \delta_\alpha^\beta$. Let $\Lambda(y) = (\Lambda_\alpha^\gamma(y))$ be the inverse matrix of $\Gamma(y)$. Then, the following is easy to see.

Lemma 5.1 *(1) If $1 \le \alpha \le r_1$, $r_1 + 1 \le \kappa \le r$, then we have*

$$\Gamma_\kappa^\alpha(y) = \Lambda_\kappa^\alpha(y) = 0, \tag{5.3}$$

i.e.,

$$\Gamma(y) = \left[\begin{array}{c|c} \Gamma_1(y) & O \\ \hline \Gamma_{21}(y) & \Gamma_2(y) \end{array} \right], \quad \Lambda(y) = \left[\begin{array}{c|c} \Lambda_1(y) & O \\ \hline \Lambda_{21}(y) & \Lambda_2(y) \end{array} \right],$$

(2) If $r_1 + 1 \le \kappa \le r$, then we have

$$\Gamma_\kappa^\nu(y',0) = \Lambda_\kappa^\nu(y',0) = \delta_\kappa^\nu, \quad \textit{i.e.}, \ \Gamma_2(y',0) = \Lambda_2(y',0) = E. \tag{5.4}$$

and

$$\frac{\partial \Gamma_\kappa^\nu}{\partial y'^\beta}(y',0) = \frac{\partial \Lambda_\kappa^\nu}{\partial y'^\beta}(y',0) = 0. \tag{5.5}$$

Let $C_{\alpha\beta}^\kappa$ be the structure constants of $\mathfrak{g}$ with respect to the basis $\{Y_\alpha\} = \{Y'_\beta, Y''_\gamma\}$, i.e., $[Y_\alpha, Y_\beta] = \sum_\kappa C_{\alpha\beta}^\kappa Y_\kappa$. Then, the following formulas concerning the functions $\Gamma_\beta^\alpha(y)$ and $\Lambda_\beta^\alpha(y)$ are derived from the fact that $\{Y_\alpha^P(y)\}$ is a family of left-invariant vector fields on G.

Lemma 5.2

$$\sum_\gamma \left(\Gamma_\alpha^\gamma \frac{\partial \Gamma_\beta^\kappa}{\partial y^\gamma} - \Gamma_\beta^\gamma \frac{\partial \Gamma_\alpha^\kappa}{\partial y^\gamma} \right) = \sum_\gamma C_{\alpha\beta}^\gamma \Gamma_\gamma^\kappa, \tag{5.6}$$

$$\frac{\partial \Lambda_\beta^\kappa}{\partial y^\alpha} - \frac{\partial \Lambda_\alpha^\kappa}{\partial y^\beta} = -\sum_{\gamma,\nu} \Lambda_\alpha^\gamma C_{\gamma\nu}^\kappa \Lambda_\beta^\nu. \tag{5.7}$$

Proof. The first formula is obtained from the relation $[Y_\alpha^P, Y_\beta^P] = \sum_\gamma C_{\alpha\beta}^\gamma Y_\gamma^P$. The second is derived from the first by noticing $\Lambda\Gamma = E$. □

5.2 Kaluza-Klein metric and the system of geodesic flow on T^*P

Now let us consider the connection form θ of the connection $\widetilde{\nabla}$. Noticing $\theta(A^P) = A$ for $\forall A \in \mathfrak{g}$, we put

$$\theta = \sum_{\alpha=1}^{r} \Big(\sum_{i=1}^{n} \theta_i^\alpha(x,y)dx^i + \sum_{\beta=1}^{r} \Lambda_\beta^\alpha(y)dy^\beta \Big) \otimes Y_\alpha. \tag{5.8}$$

Note that the property $R_g^*\theta = \mathrm{Ad}(g^{-1})\theta$ $(g \in G)$, and we put for $G \ni g \leftrightarrow (y_1, \dots, y_r)$

$$\mathrm{Ad}(g^{-1})Y_\alpha = \sum_{\beta=1}^{r} A_\alpha^\beta(y)Y_\beta \quad (\alpha = 1, \dots, r). \tag{5.9}$$

Then, we have the following.

Lemma 5.3 *Put $\bar{\theta}_i^\alpha(x) := \theta_i^\alpha(x,0)$, and we have*

$$\theta_i^\alpha(x,y) = \sum_{\beta=1}^{r} A_\beta^\alpha(y)\bar{\theta}_i^\beta(x) \quad (i = 1, \dots, n;\ \alpha = 1, \dots, r), \tag{5.10}$$

where $A_\beta^\alpha(y)$ satisfies

$$\frac{\partial A_\beta^\alpha}{\partial y^\gamma} = -\sum_{\kappa,\nu} \Lambda_\gamma^\nu C_{\nu\kappa}^\alpha A_\beta^\kappa \quad \textit{with} \quad A_\beta^\alpha(0) = \delta_\beta^\alpha, \tag{5.11}$$

and accordingly

$$\frac{\partial \theta_i^\alpha}{\partial y^\gamma} = -\sum_{\beta,\kappa} \Lambda_\gamma^\beta C_{\beta\kappa}^\alpha \theta_i^\kappa. \tag{5.12}$$

Proof. By virtue of the property:

$$\theta_{p\cdot g}\Big(\frac{\partial}{\partial x^i}\Big) = \mathrm{Ad}(g^{-1})\theta_p\Big(\frac{\partial}{\partial x^i}\Big)$$

we get (5.10). The equations (5.11) is obtained by differentiate the formula

$$\mathrm{Ad}(g(t)^{-1})Y_\alpha = \sum_{\beta=1}^{r} A_\alpha^\beta(y(t))Y_\beta$$

with respect to t for $g(t) = g \cdot \exp(tY_\gamma)$. □

From (5.8) we see that the horizontal space H_u in T_uP $(u = (x,y))$ is generated by the vectors

$$X_i^\#(x,y) := \frac{\partial}{\partial x^i} - \sum_{\alpha,\beta} \Gamma_\alpha^\beta(y)\theta_i^\alpha(x,y)\frac{\partial}{\partial y^\beta} \quad (i = 1, \dots, n).$$

The Kaluza-Klein metric $\widetilde{m}$ on P is defined by

$$(X_i^{\#}, X_j^{\#}) = m_{ij}, \quad (X_i^{\#}, Y_\alpha^P) = 0, \quad (Y_\alpha^P, Y_\beta^P) = \delta_{\alpha\beta},$$

and is represented by

$$\left.\begin{aligned} \widetilde{m}_{ij} &= \Big(\frac{\partial}{\partial x^i}, \frac{\partial}{\partial x^j}\Big) = m_{ij} + \sum_\alpha \theta_i^\alpha(x,y)\theta_j^\alpha(x,y), \\ \widetilde{m}_{i\alpha} &= \Big(\frac{\partial}{\partial x^i}, \frac{\partial}{\partial y^\alpha}\Big) = \sum_\gamma \theta_i^\gamma(x,y)\Lambda_\alpha^\gamma(y), \\ \widetilde{m}_{\alpha\beta} &= \Big(\frac{\partial}{\partial y^\alpha}, \frac{\partial}{\partial y^\beta}\Big) = \sum_\gamma \Lambda_\alpha^\gamma(y)\Lambda_\beta^\gamma(y). \end{aligned}\right\} \tag{5.13}$$

As a consequence, we get the Hamiltonian system $(T^*P, \Omega_P, \widetilde{H})$ with

$$\Omega_P = \sum_i d\xi_i \wedge dx^i + \sum_\alpha d\eta_\alpha \wedge dy^\alpha, \tag{5.14}$$

$$\begin{aligned} \widetilde{H}(x,y;\xi,\eta) = &\sum m^{ij}(x)\xi_i\xi_j - 2\sum m^{ij}(x)\theta_j^\beta(x,y)\Gamma_\beta^\alpha(y)\xi_i\eta_\alpha \\ &+ \sum \Gamma_\gamma^\alpha(y)\theta_j^\gamma(x,y)m^{ji}(x)\theta_i^\kappa(x,y)\Gamma_\kappa^\beta(y)\eta_\alpha\eta_\beta \\ &+ \sum \Gamma_\gamma^\alpha(y)\Gamma_\gamma^\beta(y)\eta_\alpha\eta_\beta. \end{aligned} \tag{5.15}$$

The Hamiltonian flow (the geodesic flow) on T^*P is governed by the canonical equation

$$\left.\begin{aligned} \dot{x}^i &= 2\sum m^{ij}\xi_j - 2\sum m^{ij}\theta_j^\beta\Gamma_\beta^\alpha\eta_\alpha, \\ \dot{y}^\alpha &= -2\sum m^{ij}\theta_j^\beta\Gamma_\beta^\alpha\xi_i + 2\sum\Gamma_\gamma^\alpha\theta_j^\gamma m^{ji}\theta_i^\kappa\Gamma_\kappa^\beta\eta_\beta + 2\sum\Gamma_\gamma^\alpha\Gamma_\gamma^\beta\eta_\beta, \\ \dot{\xi}_i &= -\sum\frac{\partial m^{kj}}{\partial x^i}\xi_k\xi_j + 2\sum\frac{\partial}{\partial x^i}(m^{kj}\theta_j^\beta)\Gamma_\beta^\alpha\xi_k\eta_\alpha \\ &\quad -\sum\Gamma_\gamma^\alpha\frac{\partial}{\partial x^i}(\theta_j^\gamma m^{jk}\theta_k^\kappa)\Gamma_\kappa^\beta\eta_\alpha\eta_\beta, \\ \dot{\eta}_\alpha &= 2\sum m^{ij}\frac{\partial}{\partial y^\alpha}(\theta_j^\gamma\Gamma_\gamma^\beta)\xi_i\eta_\beta - 2\sum m^{ji}\frac{\partial}{\partial y^\alpha}(\Gamma_\kappa^\beta\theta_j^\kappa)\theta_i^\nu\Gamma_\nu^\gamma\eta_\beta\eta_\gamma \\ &\quad -2\sum\frac{\partial\Gamma_\kappa^\beta}{\partial y^\alpha}\Gamma_\kappa^\gamma\eta_\beta\eta_\gamma. \end{aligned}\right\} \tag{5.16}$$

We can directly see that the momentum map $J(x,y;\xi,\eta)$ is invariant under the flow governed by this equation, i.e.,

$$\frac{d}{dt}J(x(t),y(t);\xi(t),\eta(t)) = \frac{d}{dt}\Big(\sum\Gamma_\alpha^\beta(y(t))\eta_\beta(t)\otimes Y^\alpha\Big) = 0$$

by virtue of Lemmas 5.2 and 5.3.

5.3 Reduced system $(P_\mu, \Omega_\mu, H_\mu)$

Now we consider the reduced system $(P_\mu, \Omega_\mu, H_\mu)$. Note that $\mathrm{Ad}^*(g)\mu = \mu$ $(\mu = \sum \mu_\alpha Y^\alpha \in \mathfrak{g}^*)$ for $\forall g \in G_\mu$, and we have the following.

Lemma 5.4 *If* $1 \le \alpha \le r$, $r_1 + 1 \le \beta \le r$, *then*

$$\sum_{\gamma=1}^{r} \mu_\gamma C^\gamma_{\alpha\beta} = 0. \tag{5.17}$$

Proof. Put $g(t) = \exp(tY''_\beta)$ $(Y''_\beta \in \mathfrak{g}_\mu)$. Then for $\forall X \in \mathfrak{g}$ we have $\langle \mu, \mathrm{Ad}(g(t))_* X \rangle = \langle \mu, X \rangle$. Differentiate this equation with respect to t, and we get $\langle \mu, [Y''_\beta, X] \rangle = 0$, which derives (5.17). □

If $(x, y; \xi, \eta) = (x, y', y''; \xi, \eta', \eta'')$ belongs to $J^{-1}(\mu)$, then it follows from (5.2) that

$$\sum_{\gamma=1}^{r} \Gamma^\gamma_\alpha(y)\eta_\gamma = \mu_\alpha \quad (\alpha = 1, \ldots, r), \tag{5.18}$$

and accordingly

$$\eta_\alpha = \sum_{\gamma=1}^{r} \Lambda^\gamma_\alpha(y)\mu_\gamma \quad (\alpha = 1, \ldots, r). \tag{5.19}$$

Thus, we can take $(x, y; \xi) = (x, y', y''; \xi)$ as local coordinates of $J^{-1}(\mu)$ in the neighborhood W of $p_0 = (x_0, 0, 0; \xi_0, \mu', \mu'')$. From (5.19) we have

$$d\eta_\alpha = \sum_{\beta,\gamma=1}^{r} \mu_\gamma \frac{\partial \Lambda^\gamma_\alpha}{\partial y^\beta} dy^\beta. \tag{5.20}$$

Therefore we have

$$\begin{aligned} i^*_\mu \Omega_P &= \sum_i d\xi_i \wedge dx^i + \frac{1}{2}\sum_\gamma \mu_\gamma \Big[\sum_{\alpha,\beta} \Big(\frac{\partial \Lambda^\gamma_\alpha}{\partial y^\beta} - \frac{\partial \Lambda^\gamma_\beta}{\partial y^\alpha}\Big) dy^\beta \wedge dy^\alpha\Big] \\ &= \sum_i d\xi_i \wedge dx^i + \frac{1}{2}\sum_{\alpha,\beta} \Big(\sum_{\gamma,\kappa,\nu} \mu_\gamma \Lambda^\kappa_\beta C^\gamma_{\kappa\nu} \Lambda^\nu_\alpha\Big) dy^\alpha \wedge dy^\beta \end{aligned}$$

on $J^{-1}(\mu)$ by virtue of (5.7). Here notice Lemmas 5.1 and 5.4, and we get

$$\begin{aligned} &(i^*_\mu \Omega_P)(x, y', y'', \xi) \\ &\quad = \sum_i d\xi_i \wedge dx^i + \frac{1}{2}\sum_{\alpha,\beta=1}^{r_1} \Big(\sum_{\kappa,\nu=1}^{r_1} \sum_{\gamma=1}^{r} \mu_\gamma \Lambda^\kappa_\beta(y) C^\gamma_{\kappa\nu} \Lambda^\nu_\alpha(y)\Big) dy'^\alpha \wedge dy'^\beta. \end{aligned}$$

Two points $(x_1, y'_1, y''_1; \xi_1)$ and $(x_2, y'_2, y''_2; \xi_2)$ are in the same G_μ-orbit if and only if $x_1 = x_2, y'_1 = y'_2, \xi_1 = \xi_2$. Hence we take $(x, y'; \xi)(= (x, y', 0; \xi))$ as local coordinates of P_μ, and have the following.

Proposition 5.5 *The symplectic form Ω_μ on P_μ is locally expressed as*

$$\begin{aligned}\Omega_\mu(x,y';\xi) &= \sum_i d\xi_i \wedge dx^i \\ &+\frac{1}{2}\sum_{\alpha,\beta=1}^{r_1}\Big(\sum_{\kappa,\nu=1}^{r_1}\sum_{\gamma=1}^{r}\mu_\gamma\Lambda^\kappa_\beta(y',0)C^\gamma_{\kappa\nu}\Lambda^\nu_\alpha(y',0)\Big)dy'^\alpha\wedge dy'^\beta. \quad (5.21)\end{aligned}$$

Remark. For a fixed $p \in T^*U$ we have the bijection $\kappa_q : \mathcal{O}_\mu \to \Phi_\mu^{-1}(q)(\subset P_\mu)$ given by $\kappa_q(q) := \Psi_u(q,\nu)$ $(\nu \in \mathcal{O}_\mu)$ (see §3). Then, the two form $\kappa_q^*\Omega_\mu$ is just the symplectic form on $\mathcal{O}_\mu$ called the *Kirillov-Kostant form*(cf. [6]). The coadjoint orbit $\mathcal{O}_\mu$ is locally parameterized by the coordinates $(y'^1,\dots,y'^{r_1})$, and the second term in (5.21) is just the Kirillov-Kostant form.

By plugging (5.18) into (5.15) we have

$$\begin{aligned}H_\mu(x,y';\xi) &= \sum_{i,j=1}^{n} m^{ij}(x)\xi_i\xi_j - 2\sum_{i,j=1}^{n}\sum_{\gamma=1}^{r} m^{ij}(x)\theta^\gamma_j(x,y',0)\xi_i\mu_\gamma \\ &+\sum_{i,j=1}^{n}\sum_{\gamma,\kappa=1}^{r}\theta^\gamma_j(x,y',0)m^{ji}(x)\theta^\kappa_i(x,y',0)\mu_\gamma\mu_\kappa + \sum_{\gamma=1}^{r}(\mu_\gamma)^2. \\ &\qquad (5.22)\end{aligned}$$

As a consequence, we get the equation of the motion in the reduced Hamiltonian system (P_μ,Ω_μ,H_μ).

Proposition 5.6 *The Hamiltonian flow on the reduced phase space P_μ is governed by*

$$\left.\begin{aligned}\dot{x}^i &= 2\sum_{i,j=1}^{n}\Big[m^{ij}(x)\xi_j - \sum_{\gamma=1}^{r} m^{ij}(x)\theta^\gamma_j(x,y',0)\mu_\gamma\Big], \\ \dot{\xi}_i &= -\sum_{j,k=1}^{n}\Big[\frac{\partial m^{kj}}{\partial x^i}\xi_k\xi_j - 2\sum_{\gamma=1}^{r}\frac{\partial}{\partial x^i}(m^{kj}\theta^\gamma_j)\xi_k\mu_\gamma \\ &\quad + 2\sum_{\gamma,\kappa=1}^{r}\frac{\partial}{\partial x^i}(m^{jk}\theta^\gamma_j)\theta^\kappa_k\mu_\gamma\mu_\kappa\Big], \\ \dot{y}'^\alpha &= -2\sum_{i,j=1}^{n}\Big[\sum_{\beta=1}^{r_1} m^{ij}\Gamma^\alpha_\beta\theta^\beta_j\xi_i - \sum_{\beta=1}^{r_1}\sum_{\gamma=1}^{r} m^{ji}\Gamma^\alpha_\beta\theta^\beta_j\theta^\gamma_i\mu_\gamma\Big] \quad (\alpha = 1,\dots,r_1).\end{aligned}\right\} \quad (5.23)$$

Proof. The Hamiltonian vector field $X_{H_\mu} = \sum(X^i\partial/\partial x^i + \Xi^i\partial/\partial\xi_i + Y^\alpha\partial/\partial y^\alpha)$ corresponding to H_μ is defined by the equation $i(X_{H_\mu})\Omega_\mu = -dH_\mu$, which directly derives the first and second equations of (5.23) and

$$\sum_{\alpha,\kappa,\nu=1}^{r_1}\sum_{\gamma=1}^{r}\mu_\gamma\Lambda^\kappa_\beta C^\gamma_{\kappa\nu}\Lambda^\nu_\alpha Y^\alpha = 2\sum_{i,j=1}^{n}\Big[\sum_{\gamma=1}^{r} m^{ij}\frac{\partial\theta^\gamma_j}{\partial y'^\beta}\xi_i\mu_\gamma - \sum_{\gamma,\sigma=1}^{r} m^{ij}\frac{\partial\theta^\gamma_j}{\partial y'^\beta}\theta^\sigma_i\mu_\gamma\mu_\sigma\Big].$$

By virtue of (5.12) we get

$$\begin{aligned}\sum_{\alpha,\kappa,\nu=1}^{r_1}\sum_{\gamma=1}^{r}\mu_\gamma\Lambda^\kappa_\beta C^\gamma_{\kappa\nu}\Lambda^\nu_\alpha\, Y^\alpha = -2\sum_{i,j=1}^{n}\Big[&\sum_{\kappa,\nu=1}^{r_1}\sum_{\gamma=1}^{r} m^{ij}\Lambda^\kappa_\beta\mu_\gamma C^\gamma_{\kappa\nu}\theta^\kappa_j\xi_i\\ &-\sum_{\kappa,\nu=1}^{r_1}\sum_{\gamma,\sigma=1}^{r} m^{ji}\Lambda^\kappa_\beta\mu_\gamma C^\gamma_{\kappa\nu}\theta^\nu_j\theta^\sigma_i\mu_\sigma\Big]\end{aligned}$$

Here, we notice that the $r_1 \times r_1$ matrices $\Lambda_1 = (\Lambda^\kappa_\beta)$ and $\widetilde{C} = (\widetilde{C}_{\kappa\nu}) = (\sum_\gamma \mu_\gamma C^\gamma_{\kappa\nu})$ are non-singular, and we get the last equation of (5.23). □

5.4 Gauge field and Wong's equation

Finally, we treat the system $(T^*M_\mu, \widetilde{\Omega}_\mu, \widetilde{H}_\mu)$, in which the curvature Θ of the connection $\widetilde{\nabla}$ appears explicitly in the equation of the motion of the charged particle. The curvature form Θ of $\widetilde{\nabla}$ is defined by

$$\Theta(X,Y) := d\theta(X,Y) + \frac{1}{2}[\theta(X),\theta(Y)]$$

for $X, Y \in T_uP$ $(u \in P)$ (see [8] for example). From (5.8) we have the local expression

$$\begin{aligned}\Theta &= \sum_{\alpha=1}^{r}\Big[\frac{1}{2}\sum_{i,j=1}^{n}\Theta^\alpha_{ij}(x,y)dx^i\wedge dx^j\Big]\otimes Y_\alpha\\ &= \sum_{\alpha=1}^{r}\Big[\frac{1}{2}\sum_{i,j=1}^{n}\Big\{\Big(\frac{\partial\theta^\alpha_j}{\partial x^i}-\frac{\partial\theta^\alpha_i}{\partial x^j}\Big)+\sum_{\beta,\gamma=1}^{r_1}C^\alpha_{\beta\gamma}\theta^\beta_i\theta^\gamma_j\Big\}dx^i\wedge dx^j\Big]\otimes Y_\alpha\end{aligned} \tag{5.24}$$

by noticing (5.7) and (5.12). Moreover since Θ satisfies $R^*_g\Theta = \mathrm{Ad}(g^{-1})\Theta$, we have

$$\Theta^\alpha_{ij}(x,y) = \sum_{\beta=1}^{r}A^\alpha_\beta(y)\bar{\Theta}^\beta_{ij}(x),$$

for $\bar{\Theta}^\beta_{ij}(x) := \Theta^\beta_{ij}(x,0)$, where

$$\bar{\Theta} = \sum_{\alpha=1}^{r}\Big[\frac{1}{2}\sum_{i,j=1}^{n}\bar{\Theta}^\alpha_{ij}(x)dx^i\wedge dx^j\Big]\otimes Y_\alpha = s^*\Theta$$

is a $\mathfrak{g}$-valued two-form on $U \subset M$ (the so-called gauge field) pulled-back by the local section $s : U \ni x \mapsto (x,0) \in U \times G \cong \pi^{-1}(U)$.

For $\mu \in \mathfrak{g}$ we define the $\mathbb{R}$-valued two-form Θ_μ on P by

$$\Theta_\mu(X,Y) := \langle \mu, \Theta(X,Y)\rangle \qquad (X, Y \in T_uP).$$

By virtue of the following lemma we can regard Θ_μ as a two-form (globally defined) on M_μ.

Lemma 5.7 $\Theta_\mu(A^P, X) = 0$ *holds for any* $A \in \mathfrak{g}_\mu$ *and* $X \in T_uP$.

Proof. Note Lemma 3.2, and we see that $\langle \mu, [\theta(A^P), \theta(X)]\rangle = 0$. In fact, we have

$$\langle \mu, [\theta(A^P), \theta(X)]\rangle = \langle \mu, [A, \theta(X)]\rangle = \langle \mu, \mathrm{ad}(A)(\theta(X))\rangle = 0$$

because $\langle \mu, \mathrm{Ad}(\exp(tA))(\cdot)\rangle = \langle \mu, \cdot\rangle$ $(t \in \mathbb{R})$. □

The one-form θ_μ on P is given by

$$\theta_\mu(x,y) = \sum_{\alpha=1}^{r} \Big(\sum_{i=1}^{n} \mu_\alpha \theta_i^\alpha(x,y) dx^i + \sum_{\beta=1}^{r} \mu_\alpha \Lambda_\beta^\alpha(y) dy^\beta \Big),$$

and we can directly check that $\mathcal{L}_{Y''^P}\theta_\mu = 0$ for $Y'' \in \mathfrak{g}_\mu$, which means that θ_μ is G_μ-invariant. We can take $(x^1, \ldots, x^n, y'^1, \ldots, y'^{r_1})$ as coordinates of M_μ. Then, the two forms $d\theta_\mu$ and Θ_μ on M_μ are represented as

$$\begin{aligned}
d\theta_\mu(x,y') &= d\theta_\mu(x,y',0) \\
&= \frac{1}{2}\sum_{i,j=1}^{n}\sum_{\gamma=1}^{r} \mu_\gamma \Big(\frac{\partial \theta_j^\gamma}{\partial x^i} - \frac{\partial \theta_i^\gamma}{\partial x^j}\Big) dx^i \wedge dx^j \\
&\quad + \sum_{i=1}^{n} \sum_{\alpha,\kappa,\nu=1}^{r_1} \sum_{\gamma=1}^{r} \mu_\gamma \Lambda_\alpha^\kappa C_{\kappa\nu}^\gamma \theta_i^\nu \, dx^i \wedge dy'^\alpha \\
&\quad - \frac{1}{2} \sum_{\alpha,\beta,\kappa,\nu=1}^{r_1} \sum_{\gamma=1}^{r} \mu_\gamma \Lambda_\alpha^\kappa C_{\kappa\nu}^\gamma \Lambda_\beta^\nu \, dy'^\alpha \wedge dy'^\beta, \\
\Theta_\mu(x,y') &= \frac{1}{2}\sum_{i,j=1}^{n}\sum_{\gamma=1}^{r} \mu_\gamma \Theta_{ij}^\gamma(x,y') dx^i \wedge dx^j \quad (\Theta_{ij}^\gamma(x,y') := \Theta_{ij}^\gamma(x,y',0))
\end{aligned}$$

by means of (5.7), (5.12) and (5.24). Let $(x, y'; \bar{\xi}, \bar{\eta}) = (x^1, \ldots, x^n, y'^1, \ldots, y'^{r_1}; \bar{\xi}_1, \ldots, \bar{\xi}_{r_1}, \bar{\eta}_1, \ldots, \bar{\eta}_{r_1})$ be canonical coordinates of T^*M_μ. Then, we have

$$\widetilde{\Omega}_\mu = \sum_{i=1}^{n} d\bar{\xi}_i \wedge dx^i + \sum_{\alpha=1}^{r_1} d\bar{\eta}_\alpha \wedge dy'^\alpha + d\theta_\mu(x,y').$$

The metric m_μ is defined by

$$(\bar{X}_i^{\#}, \bar{X}_j^{\#}) = m_{ij}, \quad (\bar{X}_i^{\#}, Y_\alpha^P) = 0, \quad (Y_\alpha^P, Y_\beta^P) = \delta_{\alpha\beta},$$

for $1 \leq i, j \leq n$, $1 \leq \alpha, \beta \leq r_1$ with

$$\bar{X}_i^{\#}(x, y') := \frac{\partial}{\partial x^i} - \sum_{\alpha,\beta=1}^{r_1} \Gamma_\alpha^\beta(y', 0)\theta_i^\alpha(x, y', 0)\frac{\partial}{\partial y'^\beta}$$

and is represented by

$$\left.\begin{aligned} (m_\mu)_{ij} &= m_{ij} + \sum_{\alpha=1}^{r_1} \theta_i^\alpha(x, y', 0)\theta_j^\alpha(x, y', 0), \\ (m_\mu)_{i\alpha} &= \sum_{\gamma=1}^{r_1} \theta_i^\gamma(x, y', 0)\Lambda_\alpha^\gamma(y', 0), \\ (m_\mu)_{\alpha\beta} &= \sum_{\gamma=1}^{r_1} \Lambda_\alpha^\gamma(y', 0)\Lambda_\beta^\gamma(y', 0). \end{aligned}\right\} \tag{5.25}$$

Hence, we get

$$\begin{aligned} \widetilde{H}_\mu(x, y'; \bar{\xi}, \bar{\eta}) = \sum m^{ij}\bar{\xi}_i\bar{\xi}_j - 2\sum m^{ij}\theta_j^\beta\Gamma_\beta^\alpha\bar{\xi}_i\bar{\eta}_\alpha \\ + \sum \Gamma_\gamma^\alpha\theta_j^\gamma m^{ji}\theta_i^\kappa\Gamma_\kappa^\beta\bar{\eta}_\alpha\bar{\eta}_\beta + \sum \Gamma_\gamma^\alpha\Gamma_\gamma^\beta\bar{\eta}_\alpha\bar{\eta}_\beta. \end{aligned} \tag{5.26}$$

By straightforward calculations we see that the flow $(x(t), y'(t); \bar{\xi}(t), \bar{\eta}(t))$ of $(T^*M_\mu, \widetilde{\Omega}_\mu, \widetilde{H}_\mu)$ satisfies the equation in the form

$$\frac{d}{dt}\bar{\eta}_\alpha = \sum_\beta F^{\alpha\beta}(x, y', \bar{\xi})\bar{\eta}_\beta \quad (1 \leq \alpha \leq r_1)$$

for some functions $F^{\alpha\beta}$. Hence, we restrict the flow on the submanifold: $\bar{\eta} \equiv 0$, (which is invariant under the flow). Then, we have the following.

Theorem 5.8 *(1) The flow of $(T^*M_\mu, \widetilde{\Omega}_\mu, \widetilde{H}_\mu)$ restricted on the submanifold: $\bar{\eta} \equiv 0$ is governed by the equation*

$$\left.\begin{aligned} \dot{x}^i &= 2\sum_{i,j=1}^{n} m^{ij}(x)\bar{\xi}_j, \\ \dot{\bar{\xi}}_i &= -\sum_{j,k=1}^{n} \frac{\partial m^{kj}}{\partial x^i}(x)\bar{\xi}_k\bar{\xi}_j - 2\sum_{j,k=1}^{n}\sum_{\gamma=1}^{r} m^{jk}(x)\mu_\gamma\Theta_{ji}^\gamma(x, y')\bar{\xi}_k, \\ \dot{y}'^\alpha &= -2\sum_{i,j=1}^{n}\sum_{\beta=1}^{r_1} m^{ij}(x)\theta_j^\beta(x, y')\Gamma_\beta^\alpha(y')\bar{\xi}_i \qquad (\alpha = 1, \dots, r_1). \end{aligned}\right\} \tag{5.27}$$

(2) The map $T^*P \to T^*M_\mu$ defined by

$$(x^1, \dots, x^n, y^1, \dots, y^r; \xi_1, \dots, \xi_n, \eta_1, \dots, \eta_r) \\ \longmapsto (x^1, \dots, x^n, y'^1, \dots, y'^{r_1}; \bar{\xi}_1, \dots, \bar{\xi}_n, \bar{\eta}_1, \dots, \bar{\eta}_{r_1})$$

with

$$\left.\begin{aligned} y'^\alpha &= y^\alpha \qquad (\alpha = 1, \dots, r_1), \\ \bar{\xi}_i &= \xi_i - \sum_{\gamma=1}^{r} \theta_i^\gamma(x, y)\mu_\gamma \qquad (i = 1, \dots, n), \\ \bar{\eta}_\alpha &= \eta_\alpha - \sum_{\gamma=1}^{r} \Lambda_\alpha^\gamma(y)\mu_\gamma \qquad (\alpha = 1, \dots, r_1) \end{aligned}\right\} \qquad (5.28)$$

induces the map $\chi_\mu : P_\mu \to T^*M_\mu$, under which the canonical equation (5.23) on P_μ is transformed to the equation (5.27).

Proof. We get the assertion by straightforward calculations. □

The equation (5.27) is (essentially same as) Wong's equation (see [14]), which describes the motion of a particle with charge $\mu \in \mathfrak{g}^*$ in the gauge field Θ with the potential θ. From (5.27) we get the following.

Corollary 5.9 *The motion of the particle with charge μ in the gauge field Θ is governed by the following equation in M_μ:*

$$\left.\begin{aligned} \ddot{x}^i + \sum_{j,k=1}^{n} \Gamma_{jk}^i(x)\dot{x}^j\dot{x}^k - 2\sum_{j,k=1}^{n}\sum_{\gamma=1}^{r} m^{ij}(x)\mu_\gamma\Theta_{jk}^\gamma(x, y')\dot{x}^k &= 0, \\ \dot{y}'^\alpha = -\sum_{j=1}^{n}\sum_{\beta=1}^{r_1} \theta_j^\beta(x, y')\Gamma_\beta^\alpha(y')\dot{x}^j \qquad (\alpha = 1, \dots, r_1), & \end{aligned}\right\} \qquad (5.29)$$

where $\Gamma_{jk}^i(x)$ denotes the Christoffel symbol defined from the Riemannian structure m on M.

6 An example - $Sp(1)$-gauge fields associated to the Hopf bundles

Let $\mathbb{H}$ be the division algebra of quaternions, i.e.,

$$\mathbb{H} = \{q = s + x\boldsymbol{i} + y\boldsymbol{j} + z\boldsymbol{k} \mid s, x, y, z \in \mathbb{R},\ \boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = \boldsymbol{ijk} = -1\}.$$

Consider the product space $\mathbb{H}^{n+1} = \{q = (q_0, q_1, \dots, q_n)\}$ with the Hermitian inner product:

$$\langle q, q' \rangle = \sum_{j=0}^{n} \bar{q}_j q'_j = \sum_{j=0}^{n} (s_j - x_j\boldsymbol{i} - y_j\boldsymbol{j} - z_j\boldsymbol{k})(s'_j + x'_j\boldsymbol{i} + y'_j\boldsymbol{j} + z'_j\boldsymbol{k}),$$

and the real inner product:

$$\langle \boldsymbol{q}, \boldsymbol{q}' \rangle_{\mathbb{R}} = \mathrm{Re}\langle \boldsymbol{q}, \boldsymbol{q}' \rangle = \sum_{j=0}^{n} (s_j s_j' + x_j x_j' + y_j y_j' + z_j z_j').$$

Note that $\mathbb{H}^{n+1}$ with $\langle \cdot, \cdot \rangle_{\mathbb{R}}$ is identified with $\mathbb{R}^{4n+4}$. Let

$$S_{[2]}^{4n+3} := \{\boldsymbol{q} \mid |\boldsymbol{q}|^2 (= \overline{\boldsymbol{q}}\boldsymbol{q}) = |q_0|^2 + \cdots + |q_n|^2 = 4\} \subset \mathbb{H}^{n+1} \cong \mathbb{R}^{4n+4}$$

be the $(4n+3)$-dimensional sphere with radius 2, and let $\widetilde{m}_0$ be the Riemannian metric on it induced from $\langle \cdot, \cdot \rangle_{\mathbb{R}}$.

A quaternion λ acts on $\mathbb{H}^{n+1}$ from right:

$$\boldsymbol{q} \cdot \lambda = (q_0, \ldots, q_n) \cdot \lambda = (q_0 \lambda, \ldots, q_n \lambda).$$

Then, the Hermitian product $\langle \cdot, \cdot \rangle$ is left invariant under this action by every unit quaternions, that is, every elements of

$$Sp(1) = \{\lambda \in \mathbb{H} \mid |\lambda| = 1\}$$

which is a three-dimensional Lie group called the symplectic group ($\cong SU(2) \cong S^3$). Thus $Sp(1)$ acts freely and isometrically on $S_{[2]}^{4n+3}$, and we get the Hopf fiber bundle:

$$Sp(1) \to S_{[2]}^{4n+3} \xrightarrow{\pi} \mathbb{H}P^n \qquad (6.1)$$

over the quaternionic projective space. The tangent bundle of $S_{[2]}^{4n+3}$ is given by

$$TS_{[2]}^{4n+3} = \{(\boldsymbol{q}, \boldsymbol{u}) \mid \boldsymbol{q} \in S_{[2]}^{4n+3}, \boldsymbol{u} \in \mathbb{H}^{n+1}, \langle \boldsymbol{q}, \boldsymbol{u} \rangle_{\mathbb{R}} = 0\}.$$

For $\boldsymbol{q} \in S_{[2]}^{4n+3}$, let $V_{\boldsymbol{q}} = (d\pi)^{-1}(0) \subset T_{\boldsymbol{q}} S_{[2]}^{4n+3}$, and it is easy to see that

$$V_{\boldsymbol{q}} = \{(\boldsymbol{q}, \boldsymbol{q}v) \mid v \in \mathbb{H}, \mathrm{Re}(v) = 0\}.$$

Let $H_{\boldsymbol{q}}$ be the orthogonal compliment of $V_{\boldsymbol{q}}$ in $T_{\boldsymbol{q}} S_{[2]}^{4n+3}$ with respect to the metric $\widetilde{m}_0$, and we have

$$T_{\boldsymbol{q}} S_{[2]}^{4n+3} = H_{\boldsymbol{q}} \oplus V_{\boldsymbol{q}}. \qquad (6.2)$$

Then, we have

$$H_{\boldsymbol{q}} = \{(\boldsymbol{q}, \boldsymbol{u}) \mid \boldsymbol{u} \in \mathbb{H}^{n+1}, \langle \boldsymbol{q}, \boldsymbol{u} \rangle = 0\}.$$

We can easily check that the horizontal space $H_{\boldsymbol{q}}$ is invariant under the $Sp(1)$ action on $S_{[2]}^{4n+3}$, and accordingly, the decomposition (6.2) defines the connection $\widetilde{\nabla}$ on the principal $Sp(1)$-bundle $\pi : S_{[2]}^{4n+3} \to \mathbb{H}P^n$. Furthermore, $\mathbb{H}P^n$ endowed with the Riemannian metric m_0 such that π is a Riemannian submersion.

Let $\mathfrak{sp}(1)$ denote the Lie algebra of $Sp(1)$. Then, $\mathfrak{sp}(1)$ consists of pure imaginary quaternions, i.e.,

$$\mathfrak{sp}(1) = \{v \in \mathbb{H} \mid \mathrm{Re}(v) = 0\} = \{v = v_1\boldsymbol{i} + v_2\boldsymbol{j} + v_3\boldsymbol{k} \mid v_1, v_2, v_3 \in \mathbb{R}\} \cong \mathbb{R}^3.$$

Note that we have the natural correspondence between the vertical space V_q and $\mathfrak{sp}(1)$.

Proposition 6.1 *The connection form θ of $\widetilde{\nabla}$ (which is a $\mathfrak{sp}(1)$-valued one-form on $S^{4n+3}_{[2]}$) is given by*

$$\theta_q(u) = \frac{1}{4}\langle q, u\rangle \in \mathfrak{sp}(1) \quad ((q,u) \in T_q S^{4n+3}_{[2]}). \tag{6.3}$$

Here, note that $\langle q, u\rangle$ belongs to $\mathfrak{sp}(1)$ because $\langle q, u\rangle_{\mathbb{R}} = 0$. By using the coordinates $(q_0, \ldots, q_n)$ in $\mathbb{H}^{n+1}$ we have

$$\theta = \frac{1}{8}\sum_{j=0}^{n}(\overline{q}_j dq_j - d\overline{q}_j\, q_j) = \frac{1}{8}(\overline{q} \cdot dq - d\overline{q} \cdot q). \tag{6.4}$$

Proof. Put $v = \theta_q(u) \in \mathfrak{sp}(1)$. Then, $u - qv$ is a horizontal vector, hence

$$0 = \langle q, u - qv\rangle = \langle q, u\rangle - \langle q, qv\rangle = \langle q, u\rangle - \langle q, q\rangle\, v = \langle q, u\rangle - 4v.$$

Therefore, we obtain (6.3). □

Let us introduce a local coordinate of $\mathbb{H}P^n$ as follows. For a point $q = (q_0, q_1, \ldots, q_n) \in S^{4n+3}_{[2]}$, denote $[q] = [q_0, q_1, \ldots, q_n] = \pi(q_0, q_1, \ldots, q_n) \in \mathbb{H}P^n$. Put $U_0 = \{[q] = [q_0, \ldots, q_n] \in \mathbb{H}P^n \mid q_0 \neq 0\}$, which is a open subset of $\mathbb{H}P^n$. Then,

$$\varphi_0 : U_0 \to \mathbb{H}^n;\ [q_0, q_1, \ldots, q_n] \mapsto (p_1, p_2, \ldots, p_n) = (q_1 q_0^{-1}, q_2 q_0^{-1}, \ldots, q_n q_0^{-1})$$

gives a local coordinate of $\mathbb{H}P^n$. Take a local section

$$s : U_0 \to S^{4n+3}_{[2]};\ p = (p_1, \ldots, p_n) \mapsto \left(\frac{2}{\sqrt{1+|p|^2}}, \frac{2p_1}{\sqrt{1+|p|^2}}, \ldots, \frac{2p_n}{\sqrt{1+|p|^2}}\right).$$

The connection form $\theta_{U_0} = s^*\theta$ on $U_0 \subset \mathbb{H}P^n$ is given by

$$\theta_{U_0} = \frac{1}{2(1+|p|^2)}\sum_{j=1}^{n}(\overline{p}_j dp_j - d\overline{p}_j\, p_j) = \frac{1}{2(1+|p|^2)}(\overline{p} \cdot dp - d\overline{p} \cdot p). \tag{6.5}$$

Let Θ be the curvature form of $\widetilde{\nabla}$, which is $\mathfrak{sp}(1)$-valued two-form on $S^{4n+3}_{[2]}$, and let $\Theta_{U_0} := s^*\Theta = d\theta_{U_0} + \theta_{U_0} \wedge \theta_{U_0}$ (a gauge field on U_0). Then, we have the following.

Proposition 6.2

$$\Theta_{U_0} = \frac{1}{(1+|p|^2)^2} \sum_{j=1}^{n} d\overline{p}_j \wedge dp_j. \tag{6.6}$$

The dual space $\mathfrak{sp}(1)^*$ of the Lie algebra $\mathfrak{sp}(1)$ is identified with $\mathfrak{sp}(1)$ by the correspondence $\mathfrak{sp}(1) \ni v \leftrightarrow v^* \in \mathfrak{sp}(1)^*$ with $v^*(w) = \langle v, w \rangle_{\mathbb{R}} = \mathrm{Re}(\overline{v}w)$ ($w \in \mathfrak{sp}(1)$). Thus we have

$$\mathfrak{sp}(1)^* = \{\nu_1 \boldsymbol{i}^* + \nu_2 \boldsymbol{j}^* + \nu_3 \boldsymbol{k}^* \mid \nu_1, \nu_2, \nu_3 \in \mathbb{R}\} \cong \mathbb{R}^3.$$

Similarly, we have

$$\begin{aligned} T^* S^{4n+3}_{[2]} &= \{(\boldsymbol{q}, \boldsymbol{u}^*) \mid (\boldsymbol{q}, \boldsymbol{u}) \in T S^{4n+3}_{[2]}\} \\ &= \{(\boldsymbol{q}, \boldsymbol{u}^*) \mid \boldsymbol{q} \in S^{4n+3}_{[2]}, \boldsymbol{u} \in \mathbb{H}^{n+1},\ \langle \boldsymbol{q}, \boldsymbol{u} \rangle_{\mathbb{R}} = 0\} \end{aligned}$$

through the inner product $\langle \cdot, \cdot \rangle_{\mathbb{R}}$.

Proposition 6.3 *The momentum map $J : T^* S^{4n+3}_{[2]} \to \mathfrak{sp}(1)^*$ is given by*

$$J(\boldsymbol{q}, \boldsymbol{u}^*) = \langle \boldsymbol{q}, \boldsymbol{u} \rangle^*. \tag{6.7}$$

Proof. Note that the vector field on $S^{4n+3}_{[2]}$ associated to $v \in \mathfrak{sp}(1)$ is given by $(\boldsymbol{q}, \boldsymbol{q}v)$. Hence, by the definition of J we have

$$\begin{aligned} \langle J(\boldsymbol{q}, \boldsymbol{u}^*), v \rangle &= \langle (\boldsymbol{q}, \boldsymbol{u}^*), \boldsymbol{q}v \rangle = \langle \boldsymbol{u}, \boldsymbol{q}v \rangle_{\mathbb{R}} \\ &= \mathrm{Re}\Big[\sum_j \overline{u}_j q_j v\Big] = \mathrm{Re}\Big[\overline{\big(\sum_j \overline{q}_j u_j\big)} \cdot v\Big] = \langle \sum_j \overline{q}_j u_j, v \rangle_{\mathbb{R}}. \end{aligned}$$

Therefore, $J(\boldsymbol{q}, \boldsymbol{u}^*) = \big(\sum_j \overline{q}_j u_j\big)^* = \langle \boldsymbol{q}, \boldsymbol{u} \rangle^*$. □

Next, we consider the (co-)adjoint action of $Sp(1)$ on $\mathfrak{sp}(1)$ (or $\mathfrak{sp}(1)^*$) and its orbit. It is easy to see that

$$\mathrm{Ad}^*(\lambda) v^* = (\mathrm{Ad}(\lambda) v)^* \quad (\lambda \in Sp(1),\ v \in \mathfrak{sp}(1)).$$

Take $\lambda = x_0 + x_1 \boldsymbol{i} + x_2 \boldsymbol{j} + x_3 \boldsymbol{k} \in Sp(1)$. Then, $[\mathrm{Ad}(\lambda^{-1})\boldsymbol{i}, \mathrm{Ad}(\lambda^{-1})\boldsymbol{j}, \mathrm{Ad}(\lambda^{-1})\boldsymbol{k}] = [\,\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\,] R_\lambda$ with R_λ being a 3×3 matrix:

$$R_\lambda = \begin{bmatrix} x_0^2 + x_1^2 - x_2^2 - x_3^2 & 2(x_0 x_3 + x_1 x_2) & 2(-x_0 x_2 + x_1 x_3) \\ 2(-x_0 x_3 + x_1 x_2) & x_0^2 - x_1^2 + x_2^2 - x_3^2 & 2(x_0 x_1 + x_2 x_3) \\ 2(x_0 x_2 + x_1 x_3) & 2(-x_0 x_1 + x_2 x_3) & x_0^2 - x_1^2 - x_2^2 + x_3^2 \end{bmatrix}.$$

Here, R_λ is an element of $SO(3)$, and $\lambda \mapsto R_\lambda$ gives a homomorphism from $Sp(1)$ onto $SO(3)$. More precisely, if $\lambda = \cos(\phi/2) + \sin(\phi/2)(v_1 \boldsymbol{i} + v_2 \boldsymbol{j} + v_3 \boldsymbol{k})$, then R_λ is the rotation about the axis $v = (v_1, v_2, v_3)$ through the angle $-\phi$. Therefore, we see that the co-adjoint orbit $\mathcal{O}_\mu$ through $\mu \in \mathfrak{sp}(1)^*$ is the sphere in $\mathfrak{sp}(1)^* \cong \mathbb{R}^3$ with the center being the origin and the radius $|\mu|$. The isotropy subgroup G_μ for $\mu = \mu_1 \boldsymbol{i}^* + \mu_2 \boldsymbol{j}^* + \mu_3 \boldsymbol{k}^*$ is given by

$$G_\mu = \left\{ \cos\psi + \frac{1}{|\mu|} \sin\psi(\mu_1 \boldsymbol{i} + \mu_2 \boldsymbol{j} + \mu_3 \boldsymbol{k}) \mid 0 \le \psi < 2\pi \right\} \cong U(1)$$

if $\mu \neq 0$, and $G_\mu = Sp(1)$ if $\mu = 0$. Suppose $\mu = c\boldsymbol{k}^*$ $(c > 0)$. Then, $G_\mu = \{\cos\psi + \sin\psi \boldsymbol{k} = e^{\psi \boldsymbol{k}} \mid 0 \le \psi < 2\pi\}$ and $\mathfrak{g}_\mu = \mathbb{R}\boldsymbol{k}$. Take $\{\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$ as a orthonormal basis of $\mathfrak{sp}(1)$, and we have local coordinates (ϕ_1, ϕ_2, ψ) of $g \in Sp(1)$ given by

$$\begin{aligned} g &= \exp(\phi_1 \boldsymbol{i} + \phi_2 \boldsymbol{j}) \exp(\psi \boldsymbol{k}) \\ &= \left\{ \cos\sqrt{\phi_1^2 + \phi_2^2} + \sin\sqrt{\phi_1^2 + \phi_2^2} \Big(\frac{\phi_1}{\sqrt{\phi_1^2 + \phi_2^2}} \boldsymbol{i} + \frac{\phi_2}{\sqrt{\phi_1^2 + \phi_2^2}} \boldsymbol{j} \Big) \right\} \\ &\qquad \times \Big(\cos\psi + \sin\psi \boldsymbol{k} \Big). \end{aligned}$$

Thus we have local coordinates $(p_1, \ldots, p_n, \phi_1, \phi_2)$ of $M_\mu = S^{4n+3}_{[2]} / G_\mu$, and can explicitely represent the equation (5.29) (or (5.27)) of the motion.

Finally, we give some remarks on the case $n = 1$, that is, the Hopf bundle $\pi : S^7 \to \mathbb{H}P^1$. Note that $\mathbb{H}P^1$ is diffeomorphic with the unit sphere $S^4 = \{(p, a) \in \mathbb{H} \times \mathbb{R} \mid |p|^2 + a^2 = 1\}$ in $\mathbb{R}^5 = \mathbb{H} \times \mathbb{R}$ by the stereographic projection

$$\mathbb{H}P^1 \supset U_0 (= \mathbb{H}) \ni p \longmapsto \Big(\frac{2p}{|p|^2 + 1}, \frac{|p|^2 - 1}{|p|^2 + 1} \Big) \in S^4 \backslash \{(0, 1)\}.$$

Furthermore, the Riemannian metric m_0 previously introduced on $\mathbb{H}P^1$ is nothing but the canonical metric on S^4. The connection given by (6.3) (or the gauge field (6.6)) is an anti-self-dual Yang-Mills connection, i.e., $*\Theta_{U_0} = -\Theta_{U_0}$ holds for Hodge's $*$ operator, and is called the *Belavin-Polyakov-Schwartz-Tyupkin anti-instanton* (cf. [2], [7]).

References

[1] R. Abraham and J. Marsden, *Foundations of Mechanics*, 2nd edition, Benjamin/Cummings (1978).

[2] M.F. Atiyah, *Geometry of Yang-Mills Fields* (Fermi Lectures), Accad. Naz. Lincei, Scuola Norm. Sup., Pisa, 1979.

[3] V. Guillemin and S. Sternberg, On the equations of motion of a particle in a Yang-Mills field and the principle of general covariance, Hadronic J., **1**(1978), 1-32.

[4] V. Guillemin and S. Sternberg, *Symplectic techniques in physics*, Cambridge Univ. Press (1984).

[5] R. Kerner, Generalization of the Kaluza-Klein theory for an arbitrary non-abelian gauge group, Ann. Inst. H. Poincaré Sect. A(N.S.), **9**(1968), 143-152.

[6] A. Kirillov, *Lectures on the Orbit Method*, Graduate Studies in Math. Vol.64, AMS (2004).

[7] S. Kobayashi, *Differential Geometry of Connections and Gauge Theory*, Shokabou(1989)(in Japanese).

[8] S. Kobayashi and K. Nomizu, *Foundations of Differential Geometry*, Vol.I, John Wiley & Sons, Inc. (Interscience Devision) (1963).

[9] M. Kummer, On the construction of the reduced phase space of a Hamiltonian system with symmetry, Indiana Univ. Math. J., **30**(1981), 281-291. 439-458.

[10] R. Kuwabara, On the classical and the quantum mechanics in a magnetic field, J. Math. Tokushima Univ., **29**(1995), 9-22; Correction and addendum, J. Math. Tokushima Univ., **30**(1996), 81-87.

[11] R. Kuwabara, Difference spectrum of the Schrödinger operator in a magnetic field, Math. Z., **233**(2000), 579-599.

[12] R. Kuwabara, Eigenvalues associated with a periodic orbit of the magnetic flow, Contemporary Math., **348**(2004), 169-180.

[13] J. Marsden and A. Weinstein, Reduction of symplectic manifolds with symmetry, Rep. Math. Phys., **5**(1974), 121-130.

[14] R. Montgomery, Canonical formulations of a classical particle in a Yang-Mills field and Wong's equations, Lett. Math. Phys., **8**(1984), 59-67.

平成17年12月15日　印刷
平成17年12月20日　発行

発行者　徳島大学　総合科学部　数理科学教室
　　　　　　　　　工学部　数学教室

編集委員　片山真一

印刷所　徳島市問屋町165番地
　　　　協業組合 徳島印刷センター