Description of our Magma codes with an example

Momonari Kudo*, Shushi Harashita† and Hayato Senda‡

November 12, 2019

Throughout, we use the same notation as in [3]. In the following, we list our Magma [1, 2] codes used for proving Theorem 4.1.1 and Proposition 4.2.1, and for the computation in Section 5 of [3]:

- "`AutPrime-N1_v2.txt`" (resp. "`AutPrime-N2_v2.txt`", "`AutPrime-Dege_v2.txt`") computes the set $G_{\mathbb{F}_{11}}$ for each of $P_i^{(\mathrm{N1})}$ (resp. $P_j^{(\mathrm{N2})}$, $P_k^{(\mathrm{Dege})}$) with $1 \leq i \leq 8$ (resp. $1 \leq j \leq 5$, $1 \leq k \leq 17$).

- "`Group_Structure_AutPrime-N1_v2.txt`" (resp. "`Group_Structure_AutPrime-N2_v2.txt`", "`Group_Structure_AutPrime-Dege_v2.txt`") determines the structure of $G_{\mathbb{F}_{11}} \cong \mathrm{Aut}_{\mathbb{F}_{11}}(C_i^{(\mathrm{N1})})$ (resp. $G_{\mathbb{F}_{11}} \cong \mathrm{Aut}_{\mathbb{F}_{11}}(C_j^{(\mathrm{N2})})$, $G_{\mathbb{F}_{11}} \cong \mathrm{Aut}_{\mathbb{F}_{11}}(C_k^{(\mathrm{Dege})})$) as abstract group, and computes generators of $G_{\mathbb{F}_{11}}$ for $1 \leq i \leq 8$ (resp. $1 \leq j \leq 5$, $1 \leq k \leq 13$).

- "`AutAC-N1_v2.txt`" (resp. "`AutAC-Dege_v2.txt`") computes the set $G^1_{\overline{\mathbb{F}_{11}}}$ for each of $P_i^{(\mathrm{alc})}$ with $1 \leq i \leq 3$ (resp. $4 \leq i \leq 9$).

- "`Group_Structure_AutAC-N1_v2.txt`" (resp. "`Group_Structure_AutAC-Dege_v2.txt`") determines the structure of $G^1_{\overline{\mathbb{F}_{11}}}/\mu_3(\overline{\mathbb{F}_{11}}) \cong \mathrm{Aut}(C_i^{(\mathrm{alc})})$ as abstract group, and computes generators of $G^1_{\overline{\mathbb{F}_{11}}}/\mu_3(\overline{\mathbb{F}_{11}})$ for $1 \leq i \leq 3$ (resp. $4 \leq i \leq 9$).

- "`ZeroDimensionalIdealVariety.txt`" contains the function

  "`ZeroDimensionalIdealVarietyOverAlgebraicClosure`".

  Given a set F of generators for a zero-dimensional ideal $I \subset K[x_1, \ldots, x_n]$, the above function computes all zeros of I over the algebraic closure $\overline{K}$.

- "`GaloisCohomology_AC_v2.txt`" conducts the computation in Section 5.

Example. We here demonstrate the computation in the proofs of Theorem 4.1.1 and Proposition 4.2.1 in [3]. In the following, assume that all program files are placed in the directory `C:/Users`. First we compute the set $G^1_{\overline{\mathbb{F}_{11}}}$ for $P_1^{(\mathrm{alc})}$ by loading the file `AutAC-N1_v2.txt`, where Algorithm 3.1.1 is implemented, together with `ZeroDimensionalIdealVariety.txt`. Before loading `AutAC-N1_v2.txt`, open it and update the forth line as follows:

*Kobe City College of Technology. E-mail: `m-kudo@math.kyushu-u.ac.jp`

†Graduate School of Environment and Information Sciences, Yokohama National University. E-mail: `harasita@ynu.ac.jp`

‡Graduate School of Environment and Information Sciences, Yokohama National University.

```
load"C:/Users/ZeroDimensionalIdealVariety.txt";
```

Here the following is a piece of the output:

```
Magma V2.22-3     Sun Nov 10 2019 16:12:52 on home19890415 [Seed = 2550300092]
Type ? for help.  Type <Ctrl>-D to quit.
> load"C:/Users/AutAC-N1_v2.txt";
========
P_{ 1 }^(alc)= x^2*y + x^2*z + x*z^2 + 4*y^3 + 2*y^2*z + 10*y^2*w + 3*y*z^2 + 8*y*z*w
 + 8*y*w^2 + 8*z^3 + 7*z^2*w + 7*z*w^2 + 4*w^3
the smallest field including all the roots of the multivariate system over algebraic
closure: Finite field of size 11^2
total roots: 36
========
M[ 1 ]:=Matrix([
[ 1, 0, 0, 0 ]
,
[ 0, 1, 0, 0 ]
,
[ 0, 0, 1, 0 ]
,
[ 0, 0, 0, 1 ]
]);
M[ 2 ]:=Matrix([
[ KK.1^40, 0, 0, 0 ]
,
[ 0, KK.1^40, 0, 0 ]
,
[ 0, 0, KK.1^40, 0 ]
,
[ 0, 0, 0, KK.1^40 ]
]);
```

... (Omitted)

```
M[ 36 ]:=Matrix([
[ KK.1^44, KK.1^44, KK.1^20, KK.1^80 ]
,
[ KK.1^8, KK.1^8, KK.1^80, KK.1^20 ]
,
[ KK.1^32, KK.1^8, KK.1^8, KK.1^44 ]
,
[ KK.1^56, KK.1^32, KK.1^8, KK.1^44 ]
]);
```

This shows that every coordinate of all the roots to each multivariate system appearing in Algorithm 3.1.1 lies in the finite fields of 11^2 elements, namely $G^1_{\overline{\mathbb{F}_{11}}} \subset \mathrm{GL}_4(\mathbb{F}_{11^2})$. The number of roots is 36, i.e., $\#G^1_{\overline{\mathbb{F}_{11}}} = 36$. The 36 elements are displayed as "`M[ i ] = `", where

"KK.1" is a primitive element of $\mathbb{F}_{11^2}$. We store the computed 36 elements in the separated file `List_of_Matrices_AutAC-N1_v2.txt`.

Next, we determine the structure of $G^1_{\overline{\mathbb{F}_{11}}}/\mu_3(\overline{\mathbb{F}_{11}}) \cong \mathrm{Aut}(C_1^{(\mathrm{alc})})$ as abstract group, and computes generators of $G^1_{\overline{\mathbb{F}_{11}}}/\mu_3(\overline{\mathbb{F}_{11}})$. Place the file `List_of_Matrices_AutAC-N1_v2.txt` in the directory `C:/Users`, before loading the file `Group_Structure_AutAC-N1_v2.txt`. In the text file `Group_Structure_AutAC-N1_v2.txt`, the group $\mu_3(\overline{\mathbb{F}_{11}})$ (resp. $G^1_{\overline{\mathbb{F}_{11}}}/\mu_3(\overline{\mathbb{F}_{11}})$) is defined as `Mu` (resp. `G/Mu`). Here the following is a piece of the output:

```
> load"C:/Users/Group_Structure_AutAC-N1_v2.txt";
Loading "C:/Kudo/Automorphism_new/Group_Structure_AutAC-N1.txt"
Loading "C:/Kudo/Automorphism_new/List_of_Matrices_AutAC-N1.txt"
=========================
P_{ 1 }^(alc)
-------------------------
Candidate for the finite group isomorphic to Aut_K (C) with C = V(Q,P):
----------
Permutation group acting on a set of cardinality 6
Order = 12 = 2^2 * 3
    (1, 2, 3, 4, 5, 6)
    (1, 6)(2, 5)(3, 4)
-------------------------
(1, 6)(2, 5)(3, 4)
|--->
[       6       3       5       3]
[       1       6       1       5]
[       5       3       6       3]
[       1       5       1       6]
Order: 2
----------
(1, 2, 3, 4, 5, 6)
|--->
[       0       6       0      10]
[       0       8       0       7]
[       1       0       2       0]
[       6       0       3       0]
Order: 6
----------
```

From the output, we have the isomorphism $G^1_K/\mu_3(\overline{\mathbb{F}_{11}}) \cong \mathrm{D}_6$, where D_6 denotes the dihedral group of degree 6. In Magma, the dihedral group D_6 is given as the subgroup of the symmetric group S_6 of degree 6 generated by the permutations $(1,6)(2,5)(3,4)$ and $(1,2,3,4,5,6)$. The isomorphism is explicitly given by

$$(1,6)(2,5)(3,4) \mapsto a := \begin{pmatrix} 6 & 3 & 5 & 3 \\ 1 & 6 & 1 & 5 \\ 5 & 3 & 6 & 3 \\ 1 & 5 & 1 & 6 \end{pmatrix}, \quad \text{and} \quad (1,2,3,4,5,6) \mapsto b := \begin{pmatrix} 0 & 6 & 0 & 10 \\ 0 & 8 & 0 & 7 \\ 1 & 0 & 2 & 0 \\ 6 & 0 & 3 & 0 \end{pmatrix},$$

whose orders are 2 and 6 respectively. Hence a and b generates $G^1_K/\mu_3(\overline{\mathbb{F}_{11}}) \cong \mathrm{Aut}(C_1^{(\mathrm{alc})})$.

References

[1] Bosma, W., Cannon, J. and Playoust, C.: *The Magma algebra system. I. The user language*, Journal of Symbolic Computation **24**, 235–265 (1997)

[2] Cannon, J., et al.: *Magma A Computer Algebra System*, School of Mathematics and Statistics, University of Sydney, 2016. `http://magma.maths.usyd.edu.au/magma/`

[3] Kudo, M., Harashita, S. and Senda, S.: *Automorphism groups of superspecial curves of genus 4 over* $\mathbb{F}_{11}$, preprint.