iSAT Benchmark: An Aircraft Collision Avoidance System

AVACS H1/2

---

1 Context and Model description

A classical case study was given by Tomlin et al. in [TPS98]. They present a conflict resolution protocol for air traffic management aiming at avoiding collisions between airplanes. The protocol works as follows: In case that the distance between two airplanes, for simplicity both remaining at the same altitude, becomes too small they perform a roundabout avoidance maneuver. Each aircraft turns 90 degrees to its right (or left) and follows a half circle. Thereafter both aircraft turn again 90 degrees thus continuing back on their original route.

The kinematic equations of each airplane in this model are given by

$$\begin{aligned}\dot{x} &= v\cos(\alpha),\\ \dot{y} &= v\sin(\alpha),\\ \dot{\alpha} &= \omega,\end{aligned}$$

where x and y model the position, v the velocity, α the angular orientation, and ω the angular velocity. In standard flight mode, ω could take an arbitrary value within certain bounds, while in the collision-avoidance mode for the angular velocities ω_1 and ω_2 of both airplanes it is required that $\omega_1 = \omega_2 = c$ for constant $c \neq 0$ holds. This constraint guarantees that both airplanes fly on a circle with the same diameter.

In [HHMWT00] HyperTech was used to show that the protocol works correctly for some fixed values for the distance when starting the roundabout maneuver (≤ 7 miles), the critical distance (≤ 5 miles), and a fixed relative orientation of both aircraft (90 degrees). If in contrast to this restriction to fixed parameters more variables are allowed, e.g. different starting orientations, the maneuver no longer guarantees safety (cf. [PC07]).

2 Encoding

In order to find counter examples to collision freedom using our iSAT algorithm [FHR+07], a predicative encoding of the transition system must be given. The following listing shows the resulting model description together with a target state in which the distance between the two planes drops below a minimum value $\sqrt{c}$. The given constants have been chosen rather arbitrarily in this model.

Note that neither the initial position nor the initial angles of the planes are constrained. This means that an unsatisfiability of the system would give a general result for all starting points and initial angles within the specified ranges.

```
--  Roundabout collision-avoidance manoeuver in air-traffic management.
--  Adapted from the protocol presented by Tomlin et al.

DECL
    -- Aircraft 1.
    define v1 = 6;              -- velocity
    float [-10.0, 10.0] p1;     -- angle
    float [0.0, 1000.0] x1;     -- x position
    float [0.0, 1000.0] y1;     -- y position

    -- Aircraft 2.
    define v2 = 6;              -- velocity
    float [-10.0, 10.0] p2;     -- angle
    float [0.0, 1000.0] x2;     -- x position
    float [0.0, 1000.0] y2;     -- y position
```

```
    -- Further declarations.
    define d = 1000000;       -- square of minimal initial distance (1000)
    define a = 160000;        -- square of alert distance (400)
    define c = 78400;         -- square of critical distance (280)
    define w = -0.02;         -- angular velocity when being in circular flight
    define m = -50.0;         -- reciprocal of w

    boole jump;
    boole cruise;
    float [0.0, 500.0] dt;
    float [0.0, 500.0] t;

INIT
    -- Initially the aircraft are at least 1000 units away from each other.
    (x1 - x2)^2 + (y1 - y2)^2 >= d;

    -- They are in cruise mode.
    !jump;
    cruise;

    -- Reset global time.
    t = 0.0;

TRANS
    jump' <-> !jump;

    -- Transition from mode 'cruise' to 'collision avoidance'.
    jump and cruise  -> (
        (x1 - x2)^2 + (y1 - y2)^2 <= a and
        !cruise' and
        dt = 0.0 and

        p1' = p1 + 1.570796 and
        x1' = x1 and
        y1' = y1 and

        p2' = p2 + 1.570796 and
        x2' = x2 and
        y2' = y2);

    -- Mode 'collision avoidance' has no outgoing transition.
    jump and !cruise -> false;

    -- Cruise mode. Angular velocity is zero, i.e. angle remains constant.
    !jump and cruise -> (
        cruise' and
        dt > 0.0 and
        (x1' - x2')^2 + (y1' - y2')^2 >= a and

        p1' = p1 and
        x1' = v1 * cos(p1) * dt + x1 and
        y1' = v1 * sin(p1) * dt + y1 and

        p2' = p2 and
        x2' = v2 * cos(p2) * dt + x2 and
        y2' = v2 * sin(p2) * dt + y2);

    -- Collision avoidance mode.
    !jump and !cruise -> (
        !cruise' and
        dt > 0.0 and
        dt * -w <= 3.1415926 and
```

```
        p1' = p1 + w * dt and
        x1' = m * [v1 * sin(p1 + w * dt) - v1 * sin(p1) + x1 * w] and
        y1' = m * [-v1 * cos(p1 + w * dt) + v1 * cos(p1) + y1 * w] and

        p2' = p2 + w * dt and
        x2' = m * [v2 * sin(p2 + w * dt) - v2 * sin(p2) + x2 * w] and
        y2' = m * [-v2 * cos(p2 + w * dt) + v2 * cos(p2) + y2 * w]);

    -- Update global time.
    t' = t + dt;

TARGET
    -- Characterization of state to be reached.
    (x1 - x2)^2 + (y1 - y2)^2 <= c;
```

This model was derived from the kinematic laws presented in the first section. A very simple trigger was implemented that starts a collision avoidance maneuver whenever the distance between the two planes decreases below a certain threshold.

3 Results

For the model given above, the following traces and statistics were generated by the prototypical implementation of the iSAT algorithm[1].

With the property that the distance between the planes should reach a value below 280 while the maneuver starts at a distance of 400, the output given in appendix A.1 is generated. From this we extract the graphical trace shown in figure 1. The runtime of the solver on this example is 36 seconds on a 2 GHz Intel Core 2 Duo.

If the property is restricted further such that a very close encounter with a distance of 50 is searched for, solving needs 101 seconds and yields the trace depicted in figure 2. This trace alongside with the entire output of the tool is given in appendix A.2.

Note that these error traces are caused by the simple hazard detection that does not compute any trajectories of the planes in order to decide whether or not the maneuver should be initiated. This simplification can however also be found in the models from [TPS98] and [PC07].

References

[FHR+07] Martin Fränzle, Christian Herde, Stefan Ratschan, Tobias Schubert, and Tino Teige. Efficient Solving of Large Non-linear Arithmetic Constraint Systems with Complex Boolean Structure. *JSAT Special Issue on SAT/CP Integration*, 1:209–236, 2007.

[HHMWT00] Thomas A. Henzinger, Benjamin Horowitz, Rupak Majumdar, and Howard Wong-Toi. Beyond HYTECH: Hybrid systems analysis using interval numerical methods. In B. Krogh and N. Lynch, editors, *Hybrid Systems: Computation and Control*, volume 1790, pages 130–144, 2000.

[PC07] André Platzer and Edmund M. Clarke. The image computation problem in hybrid systems model checking. In Alberto Bemporad, Antonio Bicchi, and Giorgio Buttazzo, editors, *Hybrid Systems: Computation and Control, 10th International Conference, HSCC 2007, Pisa, Italy, Proceedings*, volume 4416 of *Lecture Notes in Computer Science*, pages 473–486. Springer, 2007.

[TPS98] Claire J. Tomlin, George J. Pappas, and Shankar Sastry. Conflict resolution for air traffic management: A study in multi-agent hybrid systems. *IEEE Transactions on Automatic Control*, 43(4):509–521, April 1998.

[1] The prototype alongside with this and other benchmarks and a manual on its usage including a short description of the input language is available for download from `http://hysat.informatik.uni-oldenburg.de`

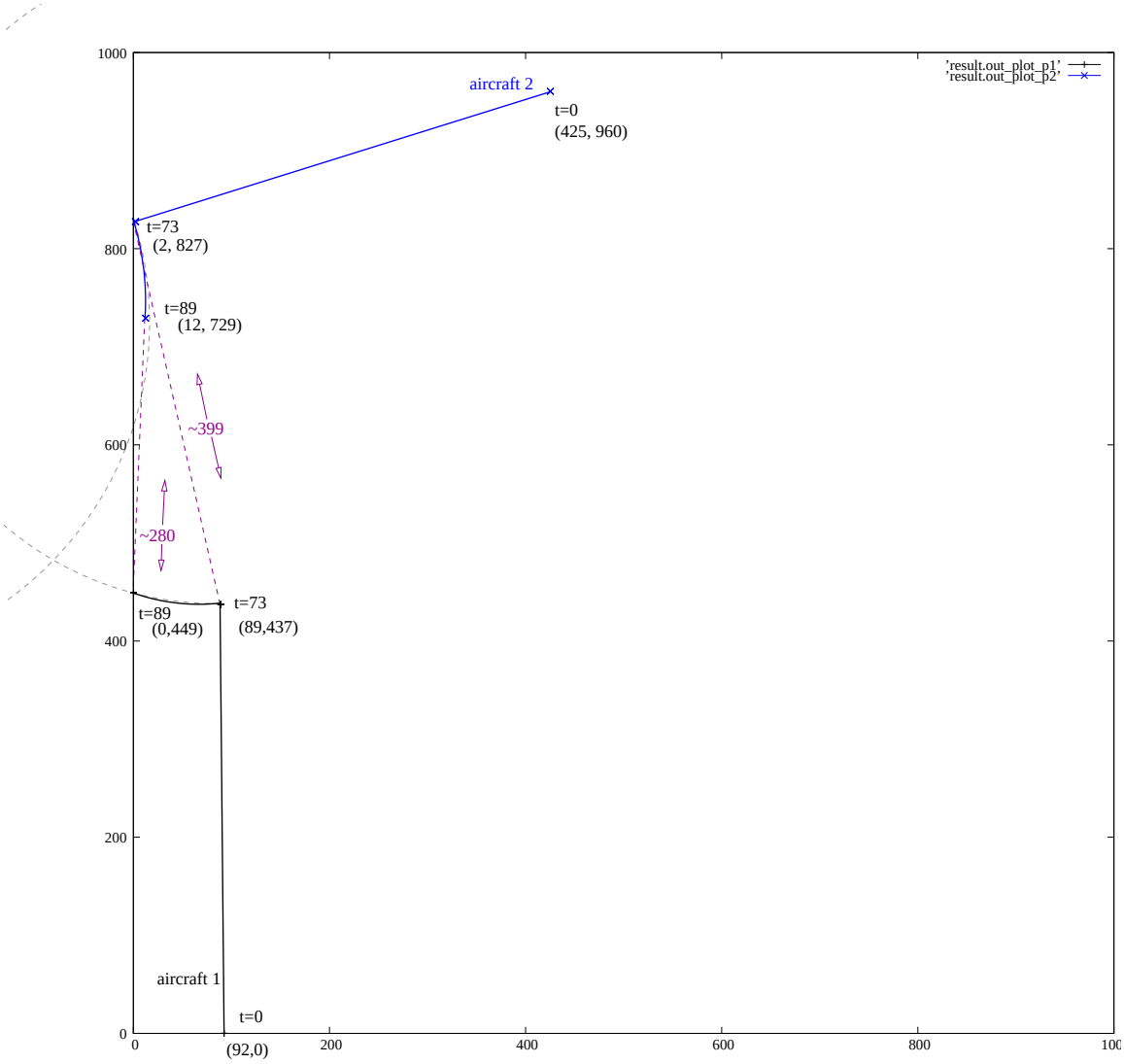

Figure 1: Trace for the medium encounter scenario with a target distance of 280 or below.

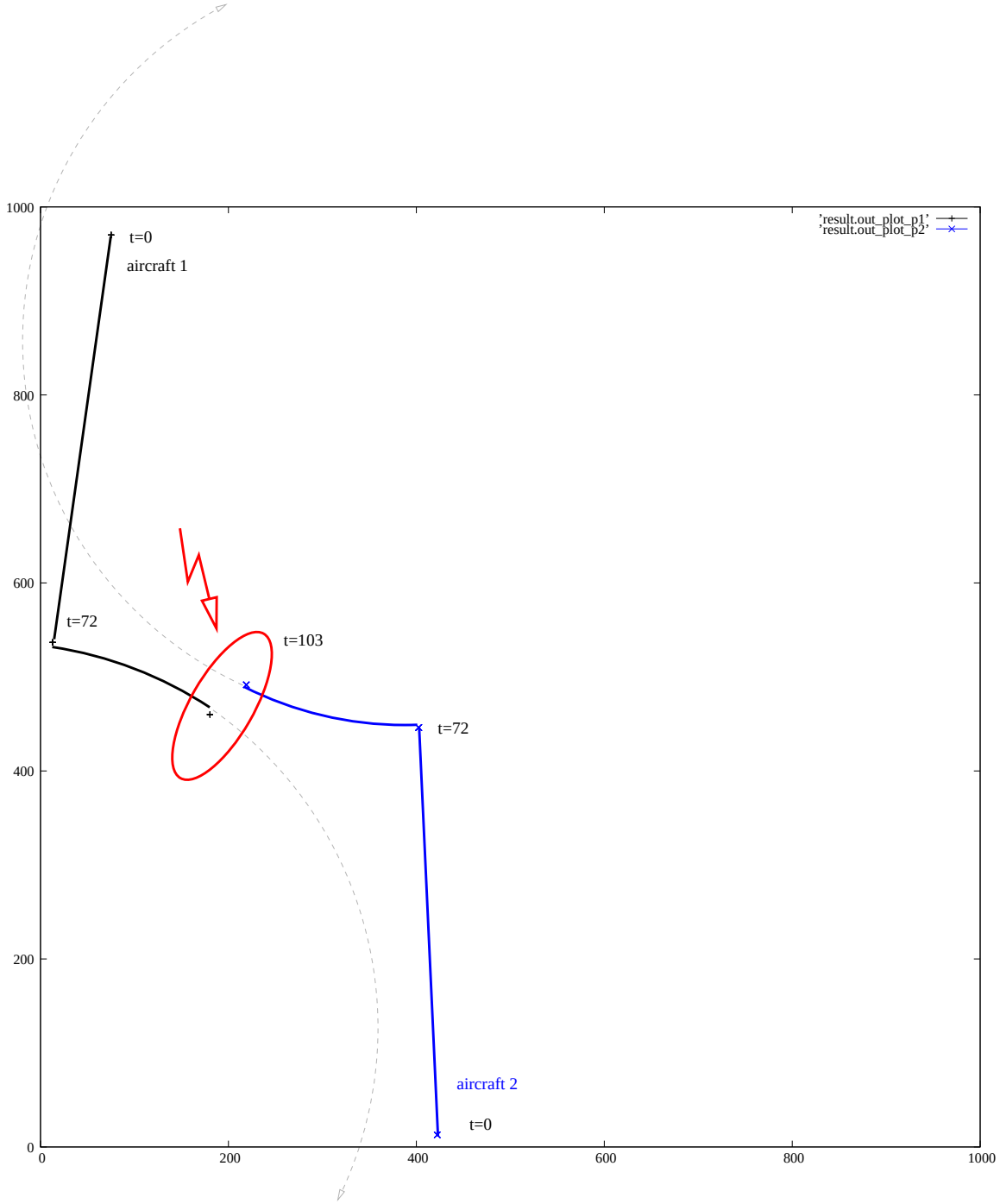

Figure 2: Trace for the close encounter scenario with a target distance of 50 or below.

A Full Output from HySAT

The output from HySAT is given entirely in the sequel for both the medium and the close encounter scenarios.

A.1 Trace 1 – medium encounter

```
# This is HySAT 0.8.1, compiled on Fri Jun 15, 2007.

Reading input file 'tomlin_aircraft_roundabout_maneuver.hys'.
Preprocessing input formulae.

SETTINGS:
    min_split_width : 0.1
    min_bound_delta : 0.01
    var_order       : standard
    reuse           : no
    shifting        : no

SOLVING:
    k = 0

RESULT:
    unsatisfiable

STATISTICS:
    num variables    : 15 (B: 3, I: 3, F: 12, C: 0)
    num dclauses     : 25 (L: 0, R: 0, T: 0, C: 0, O: 0)
    num tclauses     : 7
    num assignments  : 36 / 36
    num ineffective  : 13 / 13
    num decisions    : 0 / 0
    num conflicts    : 1 / 1
    max backjump     : 0 / 0
    max dlevel       : 0 / 0
    max dlevel depth : 37 / 37
    time solver      : 0 / 0

SOLVING:
    k = 1

RESULT:
    unsatisfiable

STATISTICS:
    num variables    : 119 (B: 19, I: 19, F: 99, C: 1)
    num dclauses     : 163 (L: 0, R: 0, T: 0, C: 0, O: 0)
    num tclauses     : 84
    num assignments  : 268 / 304
    num ineffective  : 209 / 222
    num decisions    : 0 / 0
    num conflicts    : 1 / 2
    max backjump     : 0 / 0
    max dlevel       : 0 / 0
    max dlevel depth : 304 / 304
    time solver      : 0 / 0

SOLVING:
    k = 2

RESULT:
```

```
    unsatisfiable

STATISTICS:
    num variables     : 220 (B: 35, I: 35, F: 184, C: 1)
    num dclauses      : 3859 (L: 3564, R: 0, T: 0, C: 0, O: 3564)
    num tclauses      : 161
    num assignments   : 1727471 / 1727775
    num ineffective   : 1941538 / 1941760
    num decisions     : 7383 / 7383
    num conflicts     : 3565 / 3567
    max backjump      : 33 / 33
    max dlevel        : 58 / 58
    max dlevel depth  : 71397 / 71397
    time solver       : 7.612 / 7.612

SOLVING:
    k = 3

RESULT:
    candidate solution box found

STATISTICS:
    num variables     : 321 (B: 51, I: 51, F: 269, C: 1)
    num dclauses      : 9596 (L: 9169, R: 0, T: 0, C: 0, O: 9169)
    num tclauses      : 238
    num assignments   : 5748180 / 7475955
    num ineffective   : 6161420 / 8103180
    num decisions     : 22316 / 29699
    num conflicts     : 9169 / 12736
    max backjump      : 156 / 156
    max dlevel        : 280 / 280
    max dlevel depth  : 26799 / 71397
    time solver       : 28.378 / 35.99

SOLUTION:
    cruise (boole):
        @0: [1, 1]
        @1: [1, 1]
        @2: [0, 0]
        @3: [0, 0]

    dt (float):
        @0: ]73.0426, 73.0546[
        @1: [0, 0]
        @2: ]15.948, 16.0004[

    jump (boole):
        @0: [0, 0]
        @1: [1, 1]
        @2: [0, 0]
        @3: [1, 1]

    p1 (float):
        @0: [7.86158, 7.87294]
        @1: [7.86158, 7.87189]
        @2: [9.43238, 9.44264]
        @3: [9.1118, 9.13854[

    p2 (float):
        @0: ]-2.84236, -2.8338[
        @1: ]-2.84236, -2.8338[
        @2: ]-1.28015, -1.26875]
        @3: ]-1.60074, -1.57269[
```

```
t (float):
    @0: [0, 0]
    @1: ]73.0426, 73.0546[
    @2: ]73.0426, 73.0546[
    @3: [89.0026, 89.055[

x1 (float):
    @0: [92.4492, 92.5053]
    @1: [89.1214, 89.1908]
    @2: [89.1303, 89.1908]
    @3: [0.193163, 0.254165]

x2 (float):
    @0: [425.24, 425.292[
    @1: [2.14749, 2.19908]
    @2: [2.14749, 2.19908]
    @3: [12.4637, 12.5153]

y1 (float):
    @0: [0, 0.0544456[
    @1: [437.243, 437.3]
    @2: [437.243, 437.3]
    @3: [449.339, 449.395]

y2 (float):
    @0: ]960.422, 960.476[
    @1: ]827.627, 827.681]
    @2: ]827.627, 827.681]
    @3: ]729.07, 729.125]
```

A.2 Trace 2 – close encounter

```
# This is HySAT 0.8.1, compiled on Fri Jun 15, 2007.

Reading input file 'tomlin_aircraft_roundabout_maneuver_close.hys'.
Preprocessing input formulae.

SETTINGS:
    min_split_width : 0.1
    min_bound_delta : 0.01
    var_order       : standard
    reuse           : no
    shifting        : no

SOLVING:
    k = 0

RESULT:
    unsatisfiable

STATISTICS:
    num variables    : 15 (B: 3, I: 3, F: 12, C: 0)
    num dclauses     : 25 (L: 0, R: 0, T: 0, C: 0, O: 0)
    num tclauses     : 7
    num assignments  : 36 / 36
    num ineffective  : 13 / 13
    num decisions    : 0 / 0
    num conflicts    : 1 / 1
    max backjump     : 0 / 0
    max dlevel       : 0 / 0
    max dlevel depth : 37 / 37
    time solver      : 0 / 0
```

```
SOLVING:
    k = 1

RESULT:
    unsatisfiable

STATISTICS:
    num variables     : 119 (B: 19, I: 19, F: 99, C: 1)
    num dclauses      : 163 (L: 0, R: 0, T: 0, C: 0, O: 0)
    num tclauses      : 84
    num assignments   : 268 / 304
    num ineffective   : 209 / 222
    num decisions     : 0 / 0
    num conflicts     : 1 / 2
    max backjump      : 0 / 0
    max dlevel        : 0 / 0
    max dlevel depth  : 304 / 304
    time solver       : 0 / 0

SOLVING:
    k = 2

RESULT:
    unsatisfiable

STATISTICS:
    num variables     : 220 (B: 35, I: 35, F: 184, C: 1)
    num dclauses      : 375 (L: 80, R: 0, T: 0, C: 0, O: 80)
    num tclauses      : 161
    num assignments   : 9978 / 10282
    num ineffective   : 9632 / 9854
    num decisions     : 274 / 274
    num conflicts     : 81 / 83
    max backjump      : 23 / 23
    max dlevel        : 43 / 43
    max dlevel depth  : 829 / 829
    time solver       : 0.056 / 0.056

SOLVING:
    k = 3

RESULT:
    candidate solution box found

STATISTICS:
    num variables     : 321 (B: 51, I: 51, F: 269, C: 1)
    num dclauses      : 21062 (L: 20635, R: 0, T: 0, C: 0, O: 20635)
    num tclauses      : 238
    num assignments   : 11931312 / 11941594
    num ineffective   : 14545278 / 14555132
    num decisions     : 44397 / 44671
    num conflicts     : 20635 / 20718
    max backjump      : 129 / 129
    max dlevel        : 246 / 246
    max dlevel depth  : 23154 / 23154
    time solver       : 100.562 / 100.618

SOLUTION:
    cruise (boole):
        @0: [1, 1]
        @1: [1, 1]
        @2: [0, 0]
```

```
    @3: [0, 0]

dt (float):
    @0: [72.9273, 72.9645[
    @1: [0, 0]
    @2: ]30.8677, 30.9061]

jump (boole):
    @0: [0, 0]
    @1: [1, 1]
    @2: [0, 0]
    @3: [1, 1]

p1 (float):
    @0: ]-1.7167, -1.70903[
    @1: ]-1.7167, -1.70569]
    @2: ]-0.13927, -0.130662]
    @3: ]-0.769256, -0.744297]

p2 (float):
    @0: [7.89746, 7.90652[
    @1: [7.89746, 7.90652[
    @2: [9.46826, 9.48071[
    @3: [8.84393, 8.86707[

t (float):
    @0: [0, 0]
    @1: [72.9273, 72.9645[
    @2: [72.9273, 72.9645[
    @3: ]103.795, 103.86]

x1 (float):
    @0: ]75.1444, 75.1596]
    @1: ]12.9098, 12.925[
    @2: ]12.9098, 12.925[
    @3: [180.318, 180.333[

x2 (float):
    @0: ]422.198, 422.213]
    @1: [402.533, 402.549[
    @2: [402.533, 402.549[
    @3: [219.025, 219.04[

y1 (float):
    @0: ]970.167, 970.201]
    @1: ]536.673, 536.714]
    @2: ]536.673, 536.723]
    @3: ]459.968, 460.018]

y2 (float):
    @0: ]12.8518, 12.894]
    @1: ]446.177, 446.218]
    @2: ]446.168, 446.218]
    @3: ]491.637, 491.687[
```