Modified $Prove_{ISIS}$ of BLNS code

Bianca Rampazzo

November 2025

Reordered internal pseudocode structure

Based on LaZer codebase, in particular on the structure of the functions __lnp_tbox_compute_z34 (line 1221 of lazer/src /lin-proofs.c) and lnp_quad_prove (line 9 of lazer/src /lnp-quad.c). Here I list the line numbers of the ISIS prove taken form QUBIP pdf, which must be implemented in this order. The lines containing comments are the ones that need to be modified:

```
1. ··· 6.
9.
22.
while ($b_3 == 0$){
    12.
    13.
    14.Sampling $y_3$ it's sufficient
    17.
    19.$a_1 = (t_A, t_y)$
    20.
    21.
    23.
    24.
    25.
}
15.
18.
26.$a_2 = (z_3, t_g)$
27. ··· 33.
35. ··· 40.
while ($b_1 b_2 == 0$){
    14.You need to sample $y_1, y_2$
    34.
    16.
    41.
    43.
    42.
    44.$a_4 = (t, w, f_0)$
    45. ··· 48.
}
$a_5 = (z_1, z_2)$
$\pi \leftarrow (a_1, a_2, a_3, a_4, a_5)$
```