Solve equations in Finite Fields

Notebook

Loading the package

Remember:

- The file solvefinitefield.wl must be in the same folder that your notebook file.
- You must change the directory where *Mathematica* searchs packages (to the current one).
- Typically, save first the notebook and then load the package as follows:

```
SetDirectory[NotebookDirectory[]];
```

```
<< solvefinitefield.wl
```

Examples

```
solveGF::usage
```

```
solveGF[p,n,variables,ideal] finds the solutions of
  the equations given by the ideal (without '== 0') in GF(p^n).
```

```
solveGF[2, 3, {X, Y}, {X^2 - X}]
```

```
{{X → 0, Y → 0}, {X → 0, Y → 1}, {X → 0, Y → ẋ}, {X → 0, Y → 1 + ẋ},
 {X → 0, Y → ẋ^2}, {X → 0, Y → 1 + ẋ^2}, {X → 0, Y → ẋ + ẋ^2}, {X → 0, Y → 1 + ẋ + ẋ^2},
 {X → 1, Y → 0}, {X → 1, Y → 1}, {X → 1, Y → ẋ}, {X → 1, Y → 1 + ẋ},
 {X → 1, Y → ẋ^2}, {X → 1, Y → 1 + ẋ^2}, {X → 1, Y → ẋ + ẋ^2}, {X → 1, Y → 1 + ẋ + ẋ^2}}
```

```
solveGF[2, 3, {X, Y}, {X^2 - X,  Y + 1}, False, True]
```

```
Simple solutions {Y → {1, 0, 0}_2}
Vars solved {Y}
All vars {X, Y}
Vars to solve {X}
Ideal before {1 + Y, X + X^2}
Ideal after {X + X^2}

Solutions {{X → 0, Y → {1, 0, 0}_2}, {X → {1, 0, 0}_2, Y → {1, 0, 0}_2}}
Solutions(tuple index) {1, 2}
Assignations {{0}, {0}, {{0, 1, 1}_2},
   {{0, 1, 1}_2}, {{1, 1, 0}_2}, {{1, 1, 0}_2}, {{1, 0, 1}_2}, {{1, 0, 1}_2}}
Relations {{X → 0}, {X → {1, 0, 0}_2}, {X → {0, 1, 0}_2}, {X → {1, 1, 0}_2},
   {X → {0, 0, 1}_2}, {X → {1, 0, 1}_2}, {X → {0, 1, 1}_2}, {X → {1, 1, 1}_2}}
GroebnerBasis {X + X^2}
Tuples {{0}, {{1, 0, 0}_2}, {{0, 1, 0}_2},
   {{1, 1, 0}_2}, {{0, 0, 1}_2}, {{1, 0, 1}_2}, {{0, 1, 1}_2}, {{1, 1, 1}_2}}
Elements of GF {0, {1, 0, 0}_2, {0, 1, 0}_2, {1, 1, 0}_2,
   {0, 0, 1}_2, {1, 0, 1}_2, {0, 1, 1}_2, {1, 1, 1}_2}
Ideal {-X + X^2, 1 + Y}
Variables {X}

{{X → 0, Y → {1, 0, 0}_2}, {X → {1, 0, 0}_2, Y → {1, 0, 0}_2}}
```