Inversion in a Nim tower

March 21, 2022

Grading

This homework is graded as the *contrôle continu* of this course. You must send a written report (in a portable format) **detailing** your answers to the questions 8–12 by the end of April (2022-04-29T18:00+0200) to:

pierre.karpman@univ-grenoble-alpes.fr.

This work has to be done *individually*; any fraud will be duly punished.

Unique exercise

The goal of this homework is to design an inversion algorithm for elements of $\mathbb{F}_{2^{2^n}}$ built from a recursive *Nim extension tower* as:

$$\mathbb{F}_{2^{2^n}} \cong \mathbb{F}_2[X_1, \ldots, X_n]/\langle X_i^2 + X_i + \prod_{j<i} X_j \rangle_{1 \leqslant i \leqslant n}$$

The algorithm will be recursive, which means that it will reduce arithmetic in $\mathbb{F}_{2^{2^n}}$ to arithmetic in $\mathbb{F}_{2^{2^{n-1}}}$, etc..

It can be shown that for all $n \geqslant 1$ the polynomial $X_n^2 + X_n + \prod_{j<n} X_j$ is irreducible in $\mathbb{F}_2[X_1, \ldots, X_n]/\langle X_i^2 + X_i + \prod_{j<i} X_j \rangle_{1 \leqslant i \leqslant n-1}$ (where we take the convention that for $n = 1$ the empty product equals 1), so one can build an extension of degree 2 of $\mathbb{F}_{2^{2^{n-1}}} \cong \mathbb{F}_2[X_1, \ldots, X_{n-1}]/\langle X_i^2 + X_i + \prod_{j<i} X_j \rangle_{1 \leqslant i \leqslant n-1}$ by adding one indeterminate X_n and the corresponding polynomial $X_n^2 + X_n + \prod_{j<n} X_j$ to the generators of the quotienting ideal.

Preparatory work: a multiplication algorithm

Design an addition and multiplication algorithm for the above extension tower, and analyse their cost. More precisely, answer the following:

1. How can you concisely represent "reduced" elements of $\mathbb{F}_2[X_1, \ldots, X_n]/\langle X_i^2 + X_i + \prod_{j<i} X_j \rangle_{1 \leqslant i \leqslant n}$ (*i.e.* polynomials in n variables where the degree in each indeterminate X_i is at most 1) as vectors of $\mathbb{F}_2^{2^n}$?

2. Give the vector corresponding to $X_1 + X_2 + X_1X_3 + X_2X_3$ when $n = 3$. Same question for $n = 4$.

3. How can you add together two elements of $\mathbb{F}_{2^{2^n}}$ using this embedding? Is this easy to implement on a typical CPU, when vectors are mapped to binary strings?

4. Show how to compute the multiplication of two elements $P, Q \in \mathbb{F}_{2^{2^n}}$ from four* multiplications and one *Nim transform* in $\mathbb{F}_{2^{2^{n-1}}}$ by writing them as $P = P_0 + X_n P_1$, $Q = Q_0 + X_n Q_1$, $P_0, P_1, Q_0, Q_1 \in \mathbb{F}_{2^{2^{n-1}}}$, where the Nim transform in $\mathbb{F}_{2^{2^n}}$ is the linear mapping $\mathrm{NT} : \mathbb{F}_{2^{2^n}} \cong \mathbb{F}_2[X_1, \ldots, X_n]/\langle X_i^2 + X_i + \prod_{j<i} X_j \rangle_{1 \leqslant i \leqslant n} \to \mathbb{F}_{2^{2^n}}$, $P \mapsto P \cdot X_1 \cdots X_n$.

5. Show how to recursively compute the Nim transform in $\mathbb{F}_{2^{2^n}}$ from Nim transforms in $\mathbb{F}_{2^{2^{n-1}}}$.

6. Using the same embedding into $\mathbb{F}_2^{2^n}$ as above, what is the (recursive) expression of the Nim transform as a matrix? That is, express the matrix $\boldsymbol{A}_n$ of the Nim transform in $\mathbb{F}_{2^{2^n}}$ as a block matrix in function of $\boldsymbol{A}_{n-1}$, where $\boldsymbol{A}_0 := \begin{bmatrix} 1 \end{bmatrix}$, using the convention that vectors are represented as row vectors and multiplied on their right.

7. What is the cost of this multiplication algorithm in $\mathbb{F}_{2^{2^n}}$ (using either the schoolbook or the Karatsuba algorithm in the above)? How does this compare with the addition? Hint: Use the "Master theorem" to analyse the recursivity (https://en.wikipedia.org/wiki/Master_theorem_(analysis_of_algorithms)).

An inversion algorithm

Design an inversion algorithm for the above extension tower, and analyse its cost. More precisely, answer the following:

8. Let $P = P_0 + X_n P_1 \in \mathbb{F}_{2^{2^n}}$, $P_0, P_1 \in \mathbb{F}_{2^{2^{n-1}}}$. Give $M_P \in \mathbb{F}_{2^{2^{n-1}}}^{2 \times 2}$ the matrix of multiplication by P with respect to the subfield $\mathbb{F}_{2^{2^{n-1}}}$, using the same conventions as in the above.

9. Assuming that $P \neq 0$, give an explicit formula for M_P^{-1}. Deduce an explicit formula for P^{-1} in function of P_0 and P_1.

10. Using the previous formula recursively, express the cost $\mathsf{I}(n)$ of an inversion in $\mathbb{F}_{2^{2^n}}$ from $\mathsf{I}(n-1)$, $\mathsf{M}(n-1)$, $\mathsf{N}(n-1)$, respectively the cost of inversion, multiplication and Nim transformation in $\mathbb{F}_{2^{2^{n-1}}}$.

11. Give an asymptotic formula for $\mathsf{I}(n)$, when the (naïve) algorithms of the previous questions are used for the multiplication and Nim transformation.

12. Let $\mathbb{F}$, $\mathbb{F}' \subset \mathbb{F}$ be two finite fields, $d := [\mathbb{F} : \mathbb{F}']$. The *field norm* $\mathrm{N}_{\mathbb{F}/\mathbb{F}'} : \mathbb{F} \to \mathbb{F}'$ of an element $\alpha \in \mathbb{F}$ may be defined as the determinant of the matrix of multiplication by α in $\mathbb{F}'^{d \times d}$. One of its notable properties is that it is a morphism for the field multiplication (which implies that $\mathrm{N}_{\mathbb{F}/\mathbb{F}'}(\alpha\beta) = \mathrm{N}_{\mathbb{F}/\mathbb{F}'}(\alpha)\,\mathrm{N}_{\mathbb{F}/\mathbb{F}'}(\beta)$). Use the field norm to explain in abstract terms the logic behind the inversion algorithm from the previous questions.

Remark. The tower studied in this section is a particular case of sometimes-called *Artin-Schreier towers*. Such towers play an important role (among others) in additive Fast Fourier Transform algorithms (Cantor, 1989, etc.), especially useful in characteristic two. Conway also used the above tower to define "Nim arithmetic" over the integers (and beyond); notably this allows to endow $\mathbb{N}$ with a field structure.

*Or three when using Karatsuba's algorithm.