The number of coprime/non-coprime pairs of polynomials over $\mathbb{F}_2$ with degree n and nonzero constant term

Luca Mariot
mariot@i3s.unice.fr

Enrico Formenti
enrico.formenti@unice.fr

Jean-Marc Fédou
fedou@unice.fr

September 29, 2016

Abstract

We consider the problem of counting coprime and non-coprime pairs of polynomials with binary coefficients of degree n, where both polynomials have nonzero constant term. The problem is equivalent to determining the number of pairs of orthogonal Latin squares generated by linear cellular automata, and it turns out to be connected to two known integer sequences, namely OEIS A002450 and A006095.

1 Problem Statement

Let $n \in \mathbb{N}$ be a positive integer. Define $f, g \in \mathbb{F}_2[x]$ as follows:

$$f(x) = 1 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n \ , \tag{1}$$

$$g(x) = 1 + b_1 x + \cdots + b_{n-1} x^{n-1} + x^n \ , \tag{2}$$

where $a_i, b_i \in \mathbb{F}_2$ for all $i \in \{1, \cdots, n-1\}$. In other words, f and g are polynomials with coefficients over the finite field $\mathbb{F}_2$, both of degree n and with nonzero constant term. Denote by $P_n^{1,1}$ the set of all pairs (f, g) of such polynomials. We are interested in the following problem:

Problem 1 *Define $C_n^{1,1}$ and $NC_n^{1,1}$ as the sets*

$$C_n^{1,1} = \{(f, g) \in P_n^{1,1} : \gcd(f, g) = 1\} \ , \tag{3}$$

$$NC_n^{1,1} = \{(f, g) \in P_n^{1,1} : \gcd(f, g) \neq 1\} \ . \tag{4}$$

What are the cardinalities of $C_n^{1,1}$ and $NC_n^{1,1}$?

Stated otherwise, we want to count the number of coprime and non-coprime pairs of polynomials in $P_n^{1,1}$. As remarked in [3], the problem of determining $C_n^{1,1}$ is equivalent to counting the number of pairs of orthogonal Latin squares generated by one-dimensional cellular automata with linear rules of neighborhood size n, via a characterization based on invertible Sylvester matrices.

Notice that Problem 1 has already been solved for the general case where there are no constraints on the constant terms, i.e. f and g are just two polynomials of degree n (see [6, 1]). Specifically, denoting by C_n and NC_n respectively the sets of coprime and non-coprime pairs of polynomials of degree n with any constant term, it turns out that

$$C_n = NC_n = 2^{2n-1} \quad . \tag{5}$$

The idea behind the proof (which can be generalized to any finite field $\mathbb{F}_q$) is that for each non-coprime pair $(f,g) \in NC_n$ one can construct a coprime pair $(f',g') \in C_n$ in the following way:

1. Apply Euclid's algorithm to the pair (f,g). Since (f,g) is a non-coprime pair, at the end of the algorithm the last remainder will be 0.
2. Replace the last remainder with 1, and reverse Euclid's algorithm using the same sequence of quotients computed for (f,g).
3. By construction, the pair (f',g') obtained at the end of the reverse algorithm will be coprime.

2 Counting coprime pairs by recurrence

In this section, we solve Problem 1 using a recurrence equation.

First of all, observe that the number of pairs in $P_n^{1,1}$ can be expressed as:

$$P_n^{1,1} = C_n^{1,1} + NC_n^{1,1} = C_n^{1,1} + S_n^{1,1} + DNC_n^{1,1} \quad , \tag{6}$$

where $S_n^{1,1}$ and $DNC_n^{1,1}$ respectively denote the number of symmetric pairs (f,f) in $P_n^{1,1}$ and the number of distinct non-coprime pairs in $P_n^{1,1}$.

Clearly, we have that $P_n^{1,1} = 2^{2(n-1)}$ while $S_n^{1,1} = 2^{n-1}$, since in the second case we just need to count over the central coefficients $a_1, \cdots, a_{n-1} \in \mathbb{F}_2$ of f. On the other hand, if $\gcd(f,g) \neq 1$, then the greatest common divisor of f and g has form

$$h(x) = 1 + h_1 x + \cdots + h_{d-1} + x^d \quad , \tag{7}$$

where $d \in \{1, \cdots, n-1\}$. This means that

$$f(x) = h(x) \cdot p(x) \tag{8}$$

$$g(x) = h(x) \cdot q(x) \tag{9}$$

where $(p,q) \in C_{n-d}^{1,1}$, that is, p and q are coprime polynomials of degree $n-d$ both having nonzero constant term. Since there are 2^{d-1} greatest common divisors for each degree

$d \in \{1, \cdots, n-1\}$, it follows that the number of distinct non-coprime pairs $DNC_n^{1,1}$ of degree n is given by the sum of all coprime pairs $C_{n-d}^{1,1}$ of degree $n-d \in \{1, \cdots, n-1\}$, where each term in the sum is multiplied by 2^{d-1}. In other words, it holds

$$DNC_n^{1,1} = \sum_{d=1}^{n-1} 2^{d-1} \cdot C_{n-d}^{1,1} \ . \tag{10}$$

Hence, Equation (6) can be rewritten as:

$$C_n^{1,1} = 2^{2(n-1)} - 2^{n-1} - \sum_{d=1}^{n-1} 2^{d-1} \cdot C_{n-d}^{1,1} \ . \tag{11}$$

Using Equation (11), consider now the difference between $C_n^{1,1}$ and $C_{n-1}^{1,1}$:

$$C_n^{1,1} - C_{n-1}^{1,1} = 2^{2(n-1)} - 2^{2(n-2)} - 2^{n-1} + 2^{n-2} - \sum_{d=1}^{n-1} 2^{d-1} \cdot C_{n-d}^{1,1} + \sum_{d=1}^{n-2} 2^{d-1} \cdot C_{n-1-d}^{1,1} \ . \tag{12}$$

Extracting the first term from the first sum in (12) yields

$$C_n^{1,1} - \cancel{C_{n-1}^{1,1}} = 2^{2(n-1)} - 2^{2(n-2)} - 2^{n-1} + 2^{n-2} - \cancel{2^0 \cdot C_{n-1}^{1,1}} - \sum_{d=2}^{n-1} 2^{d-1} \cdot C_{n-d}^{1,1} + \sum_{d=1}^{n-2} 2^{d-1} \cdot C_{n-1-d}^{1,1} \ . \tag{13}$$

Then, by reorganizing the terms of the two sums in Equation (13) one obtains

$$\begin{aligned} -\sum_{d=2}^{n-1} 2^{d-1} \cdot C_{n-d}^{1,1} + \sum_{d=1}^{n-2} 2^{d-1} \cdot C_{n-1-d}^{1,1} &= -2^1 \cdot C_{n-2}^{1,1} - 2^2 \cdot C_{n-3}^{1,1} - \cdots - 2^{n-2} \cdot C_1^{1,1} + \\ &\quad + 2^0 \cdot C_{n-2}^{1,1} + 2^1 \cdot C_{n-3}^{1,1} + \cdots + 2^{n-3} \cdot C_1^{1,1} = \\ &= -\sum_{d=1}^{n-2} 2^{d-1} \cdot C_{n-1-d}^{1,1} \ . \end{aligned} \tag{14}$$

which means that Equation (13) can be rewritten as

$$C_n^{1,1} = 2^{2(n-1)} - 2^{2(n-2)} - 2^{n-1} + 2^{n-2} - \sum_{d=1}^{n-2} 2^{d-1} \cdot C_{n-1-d}^{1,1} \ . \tag{15}$$

If one iterates the above procedure by subtracting $C_{n-2}, C_{n-3}, \cdots, C_1^{1,1}$ from $C_n^{1,1}$, the following result is finally obtained:

$$C_n^{1,1} = 2^{2(n-1)} - \sum_{i=0}^{n-2} 2^{2i} - 2^{n-1} + \sum_{i=0}^{n-2} 2^i \ . \tag{16}$$

The two sums in Equation (16) evaluate to the following expressions:

$$\sum_{i=0}^{n-2} 2^{2i} = \frac{4^{n-1}-1}{3} \tag{17}$$

$$\sum_{i=0}^{n-2} 2^{i} = 2^{n-1}-1 \tag{18}$$

Since $2^{2(n-1)} = 4^{n-1}$, the number of coprime pairs $C_n^{1,1}$ corresponds to:

$$C_n^{1,1} = 4^{n-1} - \frac{4^{n-1}-1}{3} - 2^{n-1} + 2^{n-1} - 1 = \left(4^{n-1}-1\right) - \frac{4^{n-1}-1}{3} = 2\cdot\frac{4^{n-1}-1}{3} \quad . \tag{19}$$

This means that the number of non-coprime pairs $NC_n^{1,1}$ is

$$NC_n^{1,1} = P_n^{1,1} - C_n^{1,1} = 4^{n-1} - 2\cdot\frac{4^{n-1}-1}{3} = \left(4^{n-1}-1\right) - 2\cdot\left(\frac{4^{n-1}-1}{3}\right) + 1 = \frac{4^{n-1}-1}{3} + 1 \quad . \tag{20}$$

Notice that formulae (19) and (20) respectively count all *ordered* coprime and non-coprime pairs of polynomials in $P_n^{1,1}$. To get the number of *distinct* coprime pairs $DC_n^{1,1}$ one simply needs to divide it by 2, thus obtaining

$$DC_n^{1,1} = \frac{4^{n-1}-1}{3} \quad . \tag{21}$$

For the number of distinct non-coprime pairs $DNC_n^{1,1}$, one has first to remove the symmetric pairs (f, f) from Equation (20) and then divide it by 2, which yields

$$DNC_n^{1,1} = \frac{1}{2}\left(\frac{4^{n-1}-1}{3} + 1 - 2^{n-1}\right) = \frac{2^{2n-3} - 3\cdot 2^{n-2} + 1}{3} = \frac{(2^{n-1}-1)(2^{n-2}-1)}{3} \quad . \tag{22}$$

Remark 1 *Let $a(n)$ be the integer sequence defined for all $n \in \mathbb{N}$ as*

$$a(n) = \frac{4^n - 1}{3} \quad .$$

This is sequence A002450 *in the OEIS [4]. It is easily seen that $a(n) = C_{n+1}^{1,1}$, i.e. $a(n)$ corresponds to the number of coprime pairs of polynomials of degree $n+1$ over $\mathbb{F}_2$ where both polynomials have nonzero constant term.*

Remark 2 *Notice that Equation* (22) *corresponds to the* Gaussian binomial coefficient $\binom{n-1}{2}_2$. *In the general case, the integer sequence corresponding to $\binom{n}{2}_2$ for $n \in \mathbb{N}$ equals*

$$b(n) = \binom{n}{2}_2 = \frac{(2^n-1)(2^{n-1}-1)}{3} \quad ,$$

which corresponds to OEIS sequence A006095 *[5]. Comparing with Equation* (22)*, it follows that $b(n) = DNC_{n+1}^{1,1}$ for all $n > 0$, i.e. $b(n)$ is the number of non-coprime pairs of polynomials of degree $n+1$ over $\mathbb{F}_2$ where both polynomials have nonzero constant term.*

Open problems

We present some open questions related to Problem 1:

- Further analyze the connection between the number of non-coprime pairs in $P_n^{1,1}$ and the Gaussian binomial coefficient. In particular, since $\binom{n-1}{2}_2$ corresponds to the number of subspaces of dimension 2 of $\mathbb{F}_2^{n-1}$ (see [2]), is it possible to describe a bijection between these subspaces and the non-coprime polynomial pairs in $P_n^{1,1}$?
- Generalize the counting result to the case of m-uples of polynomials. In particular, what is the maximum number of pairwise coprime polynomials of degree n in $P_n^{1,1}$?

References

[1] A.T. Benjamin, C.D. Bennett, The probability of relatively prime polynomials, Math. Mag. 80 (2007) 196–202

[2] P. Cameron. Enumerative Combinatorics 5: q-analogues. Lecture notes, URL: www.ltcc.ac.uk/courses/enumerative_combinatorics/l5.pdf

[3] L. Mariot, A. Leporati, E. Formenti, Constructing orthogonal Latin squares from linear cellular automata. In: Exploratory papers of AUTOMATA 2016, URL: http://openit.disco.unimib.it/~mariot/mfl_short_paper_automata_2016.pdf

[4] The Online Encyclopedia of Integer Sequences (OEIS), Sequence A002450. URL: https://oeis.org/A002450

[5] The Online Encyclopedia of Integer Sequences (OEIS), Sequence A006095. URL: https://oeis.org/A006095

[6] A. Reifegerste, On an involution concerning pairs of polynomials in $\mathbb{F}_2$, J. Combin. Theory Ser. A 90 (2000) 216–220