A CLOSED FORM EXPRESSION FOR THE DRINFE LD MODULAR POLYNOMIAL $\Phi_T(X,Y)$

ALP BASSA AND PETER BEELEN

Abstract. In this paper we give a closed form expression for the Drinfeld modular polynomial $\Phi_T(X,Y) \in \mathbb{F}_q(T)[X,Y]$ for arbitrary $q$ and prove a conjecture of Schweizer. A new identity involving the Catalan numbers plays a central role.

1. Introduction

Let $\mathbb{F}_q$ denote the finite field with $q$ elements. For a polynomial $P(T) \in \mathbb{F}_q[T]$, the Drinfeld modular polynomial $\Phi_P(X,Y) \in \mathbb{F}_q(T)[X,Y]$ defines a model for the Drinfeld modular curve $X_0(P)$. Although the Drinfeld modular polynomials play an analogously fundamental role as the classical modular polynomials, very little is known about their explicit form. For levels $P$ of low degree it is possible to compute $\Phi_P(X,Y)$ explicitly for relatively small values of $q$ only. However, even in the case $P = T$ no explicit expression for $\Phi_T(X,Y)$ is known for general $q$. The main contribution of this paper is to find such an expression for general $q$ by using a new identity involving Catalan numbers. Schweizer [6] studied $\Phi_T(X,Y)$, found an efficient algorithm to compute it for particular values of $q$ and gave two conjectures concerning its structural properties.

One of these conjectures was proven in [2], the second follows from a closed form expression for the Drinfeld modular polynomial $\Phi_T(X,Y)$ given below.

If $\phi$ is a Drinfeld module of rank two with $j$-invariant $j$ and $\phi'$ is a $P$-isogenous Drinfeld module with $j'$-invariant $j'$, then $\Phi_P(j,j') = 0$. Moreover, the function field of $X_0(P)$ is given by $\mathbb{F}_q(T)(j,j')$. Since $\phi'$ is also $P$-isogenous to $\phi$ via the dual isogeny, the Drinfeld modular polynomial is symmetric. In case $P(T)$ is an irreducible polynomial, the extension degrees $[\mathbb{F}_q(T)(j,j') : \mathbb{F}_q(T)(j)]$ and $[\mathbb{F}_q(T)(j,j') : \mathbb{F}_q(T)(j')]$ are both equal to $q^\deg P + 1$.

If $\deg P = 1$, without loss of generality we may assume that $P = T$. The genus of the Drinfeld modular curve $X_0(P)$ is zero in this case. Schweizer [4] found an explicit relation between $j, j'$ and a uniformizing parameter of the function field of $X_0(T)$. More precisely, he showed that the function field of $X_0(T)$ equals $\mathbb{F}_q(T)(z)$, where

\[ j = \frac{(z + T)^{q+1}}{z} \quad \text{and} \quad j' = \frac{(z + T^q)^{q+1}}{z^q}. \]

This implies that $\Phi_T(X,Y)$ is the unique monic, (symmetric) polynomial of degree $q + 1$ in $X$ (and $Y$), such that

\[ \Phi_T \left( \frac{(z + T)^{q+1}}{z}, \frac{(z + T^q)^{q+1}}{z^q} \right) = 0. \]

2000 Mathematics Subject Classification. Primary: 11F32, 11F52, 05A10, 11B65; Secondary: 11G09, 14G35, 11F03.

Key words and phrases. Drinfeld Modular polynomial, Catalan Numbers, Drinfeld Modular Curves.

Peter Beelen was partially supported by DNRF (Denmark) and NSFC (China), grant No.11061130539.

1
As mentioned above, in [6] an algorithm to compute $\Phi_T(X, Y)$ was given. Also a start was made to describe $\Phi_T(X, Y)$ explicitly. More precisely, writing

$$\Phi_T(X, Y) = \sum_{m=0}^{q+1} P_m(Y)X^m$$

and defining $j_0 = -T(T^{q-1} - 1)^{q+1}$ it was shown that

- $P_{q+1}(Y) = 1$
- $P_q(Y) = -(Y^q + T(Y - T^q)^{q-1} - Tq^2 + Tq - T)$
- $P_1(Y) = -Tq^2 - 2q^3 + Y(Y - j_0)^{q-1} + (Y + Tq^2 - T^q)(Tq^2 - q^2 - 1)$
- $P_0(Y) = (Y - j_0)^{q+1}$

Moreover two conjectures were formulated concerning the structure of the polynomial $\Phi_T(X, Y)$. The first conjecture concerned a closed form expression for $\Phi_T(X, Y) \mod T - 1$, which was proven to hold in [2]. The second conjecture was the following:

**Conjecture 1.** For all integers $m$ satisfying $2 \leq m \leq q - 1$ we have

$$P_m(Y) = \left( \frac{Tq(Y - j_0)}{Y - T^q} \right)^{q+1-2m}.$$

In this article we will state and prove a closed form expression for $\Phi_T(X, Y)$ (see Theorem [9]). Conjecture [11] will be a direct consequence of the closed form expression (see Corollary [10]). In the closed form the so-called Catalan numbers occur. These numbers are defined as

$$(3) \quad C_n := \frac{1}{n+1} \binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n-1}$$

and come up in a variety of combinatorial problems. In the next section we will show an identity involving Catalan numbers which is only valid in characteristic $p > 0$. This identity will play an important role in Section [3] where a proof of the closed formula of $\Phi_T(X, Y)$ is given.

### 2. An identity involving the Catalan numbers

It will be useful to extend the definition of binomial coefficients $\binom{n}{k}$ to integers $n$ and $k$:

$$(4) \quad \binom{n}{k} = \begin{cases} \frac{n(n-1) \cdots (n-k+1)}{k!} & \text{if } k \geq 0 \\ 0 & \text{otherwise.} \end{cases}$$

The following lemma is a consequences of identities (5.21) and (5.43) in [5] and will be used later.

**Lemma 1.** Let $r, m, n,$ and $\ell$ be integers and assume that $\ell \geq 0$. Then

$$(5) \quad \binom{r}{m} \binom{m}{n} = \binom{r}{n} \binom{r-n}{m-n}$$

and

$$(6) \quad \sum_{i=0}^{\ell} (-1)^i \binom{r-i}{\ell} \binom{\ell}{i} = 1.$$
Lemma 3. Let \( q = p^e \) be a power of a prime \( p \) and let \( n \) and \( k \) be integers satisfying \( n \geq 0 \) and \( n - k < q \). Then

\[
\binom{n}{k} \equiv (-1)^{n-k} \binom{q-1-k}{n-k} \pmod{p}.
\]

This lemma has the following consequence:
Lemma 4. Let \( i \) be an integer satisfying \( 0 \leq i < q - 1 \) and denote by \( C_i \) the \( i \)-th Catalan number. Then

\[
C_i \equiv (-1)^i \left( \binom{q - 1 - i}{i} + \binom{q - i}{i + 1} \right) \pmod{p}.
\]

Proof. Using equation (3) and Lemma 3 we find that

\[
C_i = \left( \frac{2i}{i} \right) - \left( \frac{2i}{i-1} \right) \equiv (-1)^i \left( \binom{q - 1 - i}{i} - (-1)^{i+1} \binom{q - i}{i + 1} \right) \pmod{p}.
\]

The result now follows. \( \square \)

We are now ready to state and prove an identity involving Catalan numbers that will turn out to be useful later.

Theorem 5. Let \( q \) be a power of a prime \( p \). Then

\[
\sum_{i=0}^{\left\lfloor \frac{q-1}{2} \right\rfloor} C_i \cdot (t(1-t))^i \equiv t^{q-1} + (1-t)^{q-1} \pmod{p}.
\]

Proof. From equation (7) we see that (in characteristic zero)

\[
\left( \frac{t}{t-1} \right)^{\frac{e+1}{2}} + \left( \frac{-1}{t-1} \right)^{\frac{e+1}{2}} = \sum_{i=0}^{\left\lfloor \frac{e+1}{2} \right\rfloor} \left( \binom{e-i}{i-1} + \binom{e-i+1}{i} \right) \left( \frac{t}{t-1} \right)^i.
\]

Replacing \( t \) by \( t/(t-1) \) we find

\[
t^{e+1} + (1-t)^{e+1} = \sum_{i=0}^{\left\lfloor \frac{e+1}{2} \right\rfloor} (-1)^i \left( \binom{e-i}{i-1} + \binom{e-i+1}{i} \right) (t(1-t))^i.
\]

Choosing \( e = q \) and using Lemma 3 we find

\[
t^{q+1} + (1-t)^{q+1} \equiv 1 - \sum_{i=1}^{\left\lfloor \frac{q+1}{2} \right\rfloor} C_{i-1} \cdot (t(1-t))^i \pmod{p}.
\]

The theorem follows directly from this. \( \square \)

Remark 6. Note that Lemma 3 implies that \( C_i \equiv 0 \pmod{p} \) for all \( i \) such that \( (q-1)/2 < i < q-1 \). This phenomenon has been observed in for example \( \text{[1]} \).

Remark 7. Note that \( t \) and \( 1-t \) are exactly the roots of the polynomial \( s^2 - s + t(1-t) \). A reformulation of equation (10) is therefore:

\[
\sum_{i=0}^{\left\lfloor \frac{q+1}{2} \right\rfloor} C_i \cdot t^i \equiv s_1^{q-1} + s_2^{q-1} \pmod{p},
\]

where \( s_1 \) and \( s_2 \) are the two roots of the polynomial \( s^2 - s + t \).

Remark 8. The generating function of the Catalan numbers \( c(x) := \sum_{i=0}^{\infty} C_i x^i \) can be expressed as

\[
c(x) = \frac{2}{1 + \sqrt{1 - 4x}}.
\]

This implies that:

\[
c(t(1-t)) = \frac{1}{1-t} = 1 + t + t^2 + \cdots.
\]
A CLOSED FORM EXPRESSION FOR THE DRINFELD MODULAR POLYNOMIAL $\Phi_T(X, Y)$

Since $c(x)$ has integer coefficients, we can reduce this relation modulo a prime number $p$ and deduce that $c(t(1-t)) \equiv 1/(1-t) \pmod{p}$. Equation (10) is a refined version of this, since it can be rewritten as

$$\sum_{i=0}^{q+1} C_i \cdot (t(1-t))^i \equiv 1 + t + \cdots + t^{q-2} + 2t^{q-1} \pmod{p}.$$  

Letting $q$ tend to infinity, but holding $p$ fixed, one recovers that $c(t(1-t)) \equiv 1/(1-t) \pmod{p}$.

3. A CLOSED FORM EXPRESSION FOR $\Phi_T(X, Y)$

Now we come to our main result:

**Theorem 9.** Let $q$ be a power of a prime $p$ and define $j_0 = -T(T^q - 1)^{q+1}$. Then

$$\Phi_T(X, Y) = (X + Y - j_0)^{q+1} - XY^q - X^qY + (XY)^q(T^{1-q} - 1) + XY(T^q - 1)^q$$

$$-T^qXY \sum_{i=0}^{q+1} C_i \cdot (XY - T^q(X + Y - j_0)^{q-1-2i}(XYT^{q+1})).$$

Equation (13) implies that the solutions to the equation

$$s_{0} = \frac{(z + T)^{q+1}}{z^q}$$

on the left-hand side in equation (12), one obtains zero.

Equation (11) implies that

$$\sum_{i=0}^{q+1} C_i \cdot \left(\frac{XYT^{q+1}}{(XY - T^q(X + Y - j_0))^2}\right)^i = s_1^{q-1} + s_2^{q-1},$$

with $s_1$ and $s_2$ equal to the two solutions to the equation

$$s^2 - s + \frac{XYT^{q+1}}{(XY - T^q(X + Y - j_0))^2} = 0.$$  

Using equation (13), one can show after some computations that

$$XY - T^q(X + Y - j_0) = \frac{(T^{q+1}(z + T)^{q-1} + z^{q+1}(z + T^q)^{q-1})(z + T)(z + T^q)}{z^{q+1}}$$

and

$$\frac{XYT^{q+1}}{(XY - T^q(X + Y - j_0))^2} = \frac{T^{q+1}(z + T)^{q-1}(z + T^q)^{q-1}}{(T^{q+1}(z + T)^{q-1} + z^{q+1}(z + T^q)^{q-1})^2}.$$  

Equation (12) implies that the solutions $s_1$ and $s_2$ to equation (15) are given by

$$s_1 = \frac{T^{q+1}(z + T)^{q-1}}{T^{q+1}(z + T)^{q-1} + z^{q+1}(z + T^q)^{q-1}}$$

and

$$s_2 = \frac{z^{q+1}(z + T^q)^{q-1}}{T^{q+1}(z + T)^{q-1} + z^{q+1}(z + T^q)^{q-1}}.$$  

Using equations \([13], [14], [10]\) and \([18]\), we find that
\[
T^{1-q}XY \sum_{i=0}^{q+1} C_i \cdot (XY - T^q(X + Y - j_0))^{q-1-2i}(XYT^{q+1})^i
\]
\[=
T^{1-q}XY(Y - T^q(X + Y - j_0))^{q-1} \sum_{i=0}^{q+1} C_i \cdot \left(\frac{XYT^{q+1}}{(XY - T^q(X + Y - j_0))^2}\right)^i
\]
\[=
T^{1-q}(z + T)^{2q}(z + T^q)^{2q} \frac{(T^{q+1}(z + T)^{q-1})^{q-1} + (z^{q+1}(z + T)^{q-1})^{q-1}}{T^{q-1}z^{q+1}}.
\]
However, a straightforward computation shows that, still with \(X\) and \(Y\) as in equation \([13]\),
\[
(X + Y - j_0)^{q+1} - XY^q - X^qY + (XY)^q(T^{1-q} - 1) + XY(T^{q-1} - 1)^2
\]
\[=
T^{q-1}(z + T)^{q+1}(z + T^q)^{2q} + (z + T)^{2q}(z + T^q)^{q+1}.
\]
This finishes the proof.

We will now prove Conjecture \([10]\) as a corollary to Theorem \([9]\).

**Corollary 10.** Define for \(0 \leq m \leq q+1\) polynomials \(P_m(Y) \in \mathbb{F}_q[T, Y]\) by the identity
\[
\Phi_T(X, Y) = \sum_{m=0}^{q+1} P_m(Y)X^m.
\]
Then for all \(m\) such that \(2 \leq m \leq q - 1\) we have
\[
\frac{P_m(Y)}{P_{q+1-m}(Y)} = \left(\frac{T^q(Y - j_0)}{Y - T^q}\right)^{q+1-2m}.
\]

**Proof.** Note that the expression \((X + Y - j_0)^{q+1} - XY^q - X^qY + (XY)^q(T^{1-q} - 1) + XY(T^{q-1} - 1)^2\)
only contributes to \(P_m(Y)\) if \(m \in \{0, 1, q, q+1\}\). Now let \(m\) be an arbitrary integer between \(2\) and \(q-1\). Since \(XY - T^q(X + Y - j_0) = X(Y - T^q) - T^q(Y - j_0)\), we see from Theorem \([9]\) that the coefficient of \(X^m\) in \(\Phi_T(X, Y)\) is given by
\[
P_m(Y) = T^{1-q}Y \sum_{i=0}^{q+1} C_i \cdot \left(\frac{q - 1 - 2i}{m - 1 - i}\right)^i(Y - T^q)^{m-1-i}(-T^q(Y - j_0))^{q-1}(T^{q+1}Y)^i
\]
\[=
T^{1-q}Y \left(\frac{Y - T^q}{-T^q(Y - j_0)}\right)^m \sum_{i=0}^{q+1} C_i \cdot \left(\frac{q - 1 - 2i}{m - 1 - i}\right)^i\left(\frac{-T^q(Y - j_0))^{q-1}(T^{q+1}Y)^i}{(Y - T^q)^{1+i}}\right).
\]
Since
\[
\left(\frac{q - 1 - 2i}{m - 1 - i}\right) = \left(\frac{q - 1 - 2i}{(q + 1 - m) - 1 - i}\right),
\]
we see that
\[
\frac{P_m(Y)}{P_{q+1-m}(Y)} = \left(\frac{(Y - T^q)/(-T^q(Y - j_0))}{(Y - T^q)/(-T^q(Y - j_0))}\right)^m.
\]
The corollary now follows directly.

**Remark 11.** Using Lemma 4 and Theorem 9, it is possible to give a closed form expression for $\Phi_T(X, Y)$ not involving the Catalan numbers. However, the resulting expression is not more compact nor easier to prove, as far as the authors know.

**Remark 12.** Setting $t = x^{q-1}/(1 + x^{q-1}) \in \mathbb{F}_q(x)$ in equation (10) one obtains after some manipulations an algebraic dependency between $u = x^q + x \in \mathbb{F}_q(x)$ and $v = x^{q+1}/(x^q + x) \in \mathbb{F}_q(x)$, namely

$$u^q \equiv u^{q-1}v^q + v + v \sum_{i=0}^{q-1} C_i u^{q-1-i}v^i \pmod{p}.$$  

The functions $u$ and $v$ occur in a natural way when defining a certain asymptotically optimal tower [4]. This tower was in [3] shown to have a Drinfeld modular interpretation. This again shows that equation (10) plays a role in the theory of Drinfeld modular curves.

**References**

[1] R. Alter and K.K. Kubota, Prime and prime power divisibility of Catalan numbers, Journal of Combinatorial Theory Series A 15, pp. 243-256 (1973).
[2] A. Bassa and P. Beelen, A proof of a conjecture by Schweizer on the Drinfeld modular polynomial $\Phi_T(X, Y)$, Journal of Number Theory 131, pp. 1276–1285 (2011).
[3] N.D. Elkies, Explicit towers of Drinfeld modular curves, Progress in Mathematics 202, pp. 189–198 (2001).
[4] A. Garcia and H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, Journal of Number Theory 61, pp. 248–273 (1996).
[5] R.L. Graham, D.E. Knuth and O. Patashnik, Concrete Mathematics, Addison-Wesley Publishing Company, 1989.
[6] A. Schweizer, On the Drinfeld Modular Polynomial $\Phi_T(X, Y)$, Journal of Number Theory 52, pp. 53–68 (1995).