ON THE GRAPH ATTACHED TO TRUNCATED BIG WITT VECTORS

NICHOLAS M. KATZ

Warning to the reader

After this paper was written, we became aware of S.D.Cohen's 1998 result [C-Graph, Theorem 1.4], which is both sharper and more general than the result, Theorem 1.1, of this paper. We leave this manuscript up only because its techniques, quite different from those of Cohen, may conceivably be of some independent interest.

1. Introduction

For any ring A, the group $BigWitt(A)$ is simply the abelian group $1+XA[[X]]$ of formal series with constant term 1, under multiplication of formal series. In this group, the elements $1 + X^{n+1}A[[X]]$ form a subgroup; the quotient by this subgroup is $BigWitt_n(A)$:

$$BigWitt_n(A) := (1 + XA[[X]])/(1 + X^{n+1}A[[X]]).$$

For each element $a \in A$, we have the element $1+aX \in BigWitt_n(A)$. Some natural questions[1] are

(1) Do the elements $\{1+aX\}_{a\in A}$ generate the group $BigWitt_n(A)$?
(2) If the answer to (1) is yes, is there an upper bound N for the number of factors $1+aX \in BigWitt_n(A)$ needed to write every element as a product of these factors? If so, what is that upper bound?

Let us form the directed graph $\mathcal{G}(n, A)$ whose vertices are the elements of $BigWitt_n(A)$, and in which there is a directed edge from the element α to the element β precisely when $\beta/\alpha = 1 + aX$ for some $a \neq 0, a \in A$. Then question (1) above asks whether this graph is connected, and question (2) asks, in cases when this graph is connected, whether it has finite diameter, and, if so, what is the diameter.

Even in the case that A is a field, the graph $\mathcal{G}(n, A)$ need not be connected if the field is too small. For example, take for A the field $\mathbb{F}_2$ of two elements. Then we are asking if $BigWitt_n(\mathbb{F}_2)$ is the cyclic

[1]Of course these questions are trivial for $n = 1$, where the answers are yes, with $N = 1$. See [Ka-FP] for the étale variant of these questions.

group generated by $1+X$. But for $n \geq 3$, the group $BigWitt_n(\mathbb{F}_2)$ is not cyclic. Already the quotient $BigWitt_3(\mathbb{F}_2)$ is not cyclic (indeed it is the product $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$).

When A the field $\mathbb{R}$ of real numbers, there are archimedean obstructions which prevent $BigWitt_2(\mathbb{R})$ from being connected for $n \geq 2$. Already in $BigWitt_2(\mathbb{R})$, the element $1+X^2$ is not a finite product of elements $1+a_iX$ with real a_i. Indeed, as we will explain below, no element of $BigWitt_2(\mathbb{R})$ of the form $1+s_1X+s_2X^2$ with $s_1^2 < 2s_2$ is such a product.

To see this last assertion, and to formulate the general framework we will use to analyze such questions, we proceed as follows. Given an integer $N \geq 1$, and N variables $a_1, ..., a_N$, we have the elementary symmetric functions $s_i(a_1, ..., a_N) \in \mathbb{Z}[a_1, ..., a_N]$, $1 \leq i \leq N$, defined by the identity

$$\prod_{i=1}^{N}(1+a_iX) = 1 + \sum_{i=1}^{N} s_i(a_1, ..., a_N)X^i$$

in $\mathbb{Z}[a_1, ..., a_N][X]$. We also have the Newton symmetric functions $N_i((a_1, ..., a_N) \in \mathbb{Z}[a_1, ..., a_N]$, $i \geq 1$, defined by the power sums

$$N_i(a_1, ..., a_N) = \sum_{j=1}^{N} a_j^i,$$

and the well known identities relating the N_i's and the s_i's. As polynomials in the a_i's, both s_j and N_j are homogeneous of degree j. For any integer $1 \leq n \leq N$, we have

$$\mathbb{Z}[N_1, ..., N_n] \subset \mathbb{Z}[s_1, ..., s_n] \text{ inside } \mathbb{Z}[a_1, ..., a_N]$$

and

$$\mathbb{Z}[1/n!][N_1, ..., N_n] = \mathbb{Z}[1/n!][s_1, ..., s_n] \text{ inside } \mathbb{Z}[1/n!][a_1, ..., a_N].$$

For any ring A, to write an element $1+\sum_{i=1}^{n} b_iX^i$ of $BigWitt_n(A)$ as the product of $N \geq n$ factors $1+a_iX$ is to solve, in A, the n equations

$$s_i(a_1, ..., a_N) = b_i,\ 1 \leq i \leq n.$$

To say that every element can be so written is to say that these n equations have A-valued solutions $(a_1, ..., a_N)$ for every n-tuple of b_i's.

When the integer $n!$ is invertible in A, these n equations have A-valued solutions $(a_1, ..., a_N)$ for every n-tuple of b_i's if and only the n equations

$$N_i(a_1, ..., a_N) = c_i,\ 1 \leq i \leq n$$

have A-valued solutions $(a_1, ..., a_N)$ for every n-tuple of c_i's.

Returning to the case when $A = \mathbb{R}$, we use the relations $N_1 = s_1, N_2 = s_1^2 - 2s_2$ and the observation that $N_2(a_1, ..., a_N) \geq 0$ whenever the a_i are all real, to justify our assertion that $\mathcal{G}(2, \mathbb{R})$ is not connected.

We will prove the following theorem.

Theorem 1.1. *Given an integer $n \geq 1$, there are explicit constants $C_2(n)$ and $C_3(n)$ such that we have the following results.*

1. *If k is a finite field with $\#k \geq C_2(n)$ whose characteristic p does not divide $(n+2)(n+1)$, then $\mathcal{G}(n,k)$ is connected, and has diameter $\leq n+2$.*
2. *If n is even, and if k is a finite field of characteristic 2 with $\#k \geq C_3(n)$, then $\mathcal{G}(n,k)$ is connected, and has diameter $\leq n+3$.*

Corollary 1.2. *Given $n \geq 1$, if k is a finite field of odd characteristic with $\#k \geq$ Max $(C_2(n), C_2(n+1), C_2(n+2))$, then $\mathcal{G}(n,k)$ is connected, and has diameter $\leq n+4$. if if k is a finite field of characteristic 2 with $\#k \geq$ Max $(C_3(n), C_3(n+1))$, then $\mathcal{G}(n,k)$ is connected, and has diameter $\leq n+4$.*

Proof. The group $BigWitt_n(k)$ is a quotient of $BigWitt_{n+1}(k)$. Hence if $\mathcal{G}(n+1,k)$ is connected, then so is $\mathcal{G}(n,k)$, and diameter$(\mathcal{G}(n,k)) \leq$ diameter$(\mathcal{G}(n+1,k))$. If p is odd, then either p does not divide $(n+2)(n+1)$, or it does not divide $(n+3)(n+2)$, or it does not divide $(n+4)(n+3)$, and we apply part (1) of the above theorem to the appropriate one of $\mathcal{G}(n,k)$, $\mathcal{G}(n+1,k)$, or $\mathcal{G}(n+2,k)$. If $p = 2$, then either n or $n+1$ is even, and we apply part (2) to the appropriate one of $\mathcal{G}(n,k)$ or $\mathcal{G}(n+1,k)$. □

Another corollary is this.

Corollary 1.3. *Given $n \geq 1$, if k is a finite field of characteristic $p \geq n+3$ with $\#k \geq C_2(n)$, then $\mathcal{G}(n,k)$ is connected, and has diameter $\leq n+2$.*

2. Proof of Theorem 1.1

Given integers $N = n + d \geq n \geq 1$, a finite field k of characteristic p, and an $n+d$ tuple $\vec{b} = (b_1, ..., b_{n+d}) \in k^{n+d}$, we define a projective variety $X(n, d, \vec{b}) \subset \mathbb{P}^{n+d}/k$ by the n homogeneous equations (in the homogeneous coordinates $a_1, ..., a_{n+d}, z$)

$$s_i(a_1, ..., a_{n+d}) = b_i z^i,\ 1 \leq i \leq n.$$

We define the affine variety $U(n,d,\vec{b}) \subset \mathbb{A}^{n+d}/k$ by the n equations (in the coordinates $a_1,...,a_{n+d}$)

$$s_i(a_1,...,a_{n+d}) = b_i,\ 1 \le i \le n.$$

We define the projective variety $Z(n,d) \subset \mathbb{P}^{n+d-1}/k$ by the n homogeneous equations (in the homogeneous coordinates $a_1,...,a_{n+d}$)

$$s_i(a_1,...,a_{n+d}) = 0,\ 1 \le i \le n.$$

Lemma 2.1. *We have the following results about the k-scheme $Z(n,d)$.*

(1) *For $d \ge 0$, $Z(n,d)$ is a complete intersection of dimension $d-1$.*
(2) *If p does not divide $(n+2)(n+1)$, $Z(n,2)$ is a smooth complete intersection curve.*
(3) *If $p = 2$ and $n+3$ is odd, $Z(n,3)$ is a complete intersection surface with at worst isolated singularities.*

Proof. If we impose d more equations $s_j = 0$ for $j = n+1,...,d+n$, the only affine solution with values in a field is $a_i = 0$ for all i (i.e. we are asking for the roots of the polynomial X^{n+d}), so the projective variety we get by imposing these d additional equations is empty. This shows that $Z(n,d)$ is a complete intersection of dimension $d-1$.

The singular locus is defined by the vanishing of all $n \times n$ minors of the $n \times (n+d)$ matrix $(\partial s_i/\partial a_j)_{1\le i\le n, 1\le j\le n+d}$. We have the following determinant formula, due to F.A. Tarleton in 1867, cf. [T], [Muir-III, page 142], [Sc, page 102], [La-Pr, page170].

Lemma 2.2. *The determinant of the $n\times n$ matrix $(\partial s_i/\partial a_j)_{1\le i\le n, 1\le j\le n}$ is*[2]

$$\pm \prod_{1\le i<j\le n} (a_i - a_j).$$

Proof. We have the identity

$$\partial s_i/\partial a_j = s_{i-1}(\text{all variables except } a_j),$$

with the convention that $s_0 = 1$. So if $a_i = a_j$ with $i \ne j$, then the matrix in question has two identical columns. Thus the determinant is divisible by $a_i - a_j$, for all $1 \le i < j \le n$, in $\mathbb{Z}[a_1,...,a_{n+d}]$, and hence is divisible by $\prod_{1\le i<j\le n}(a_i - a_j)$. On the other hand, this determinant is homogeneous in the a_j of the same degree $n(n-1)/2$, so the determinant is of the form (some integer)$\times \prod_{1\le i<j\le n}(a_i - a_j)$. If this integer factor were not ± 1, then in some finite characteristic p this determinant would vanish identically. But this is not the case. To see this, put $a_{n+1} = ... = a_{n+d} = 0$, and choose n distinct elements

[2]In fact, the sign is +, cf. [La-Pr, page170], but we do not need this finer fact.

$\alpha_j, 1 \leq j \leq n$ in some (large enough) field k of characteristic p, and take $\beta_i := s_i(\alpha_1, ..., \alpha_n)$. Then the equations

$$s_j(a_1, ..., a_n, 0, ..., 0) = \beta_j, 1 \leq j \leq n$$

define a finite étale k-scheme, hence the matrix in question is invertible at the point $(\alpha_1, ..., \alpha_n, 0..., 0)$. □

From Tarleton's determinant formula, applied to each $n \times n$ minor, we see that the geometric points $(a_1, ..., a_{n+d})$ of the singular locus are those points such that there are at most $n-1$ distinct values among the a_i.

Suppose now that p does not divide $(n+2)(n+1)$. If $(a_1, ..., a_{n+2})$ is a geometric point of the singular locus of $Z(n, 2)$, then some a_i is nonzero, there are at most $n-1$ distinct values among the a_i, and we have the polynomial identity

$$\prod_{i=1}^{n+2}(1 + a_i X) = 1 + AX^{n+1} + BX^{n+2}$$

for

$$A := s_{n+1}(a_1, ..., a_{n+2}),\ B := s_{n+2}(a_1, ..., a_{n+2}).$$

Equivalent to this identity is the palindromic identity in the variable $T := 1/X$,

$$\prod_{i=1}^{n+2}(T + a_i) = T^{n+2} + AT + B.$$

So the asserted nonsingularity in (2) results from the following elementary lemma.

Lemma 2.3. *Let $n \geq 1$ be an integer, K an algebraically closed field in which $(n+2)(n+1)$ is invertible, and $A, B \in K$. Then the polynomial $T^{n+2} + AT + B$ has either $n+1$ or $n+2$ distinct roots in K unless $A = B = 0$ (in which case its only root is 0, with multiplicity $n+2$).*

Proof. Let us write $f(T) := T^{n+2} + AT + B$. A multiple root of f is a common root of $f(T)$ and of its derivative $f'(T) = (n+2)T^{n+1} + A$. If $A = 0$, the only root of f' is 0, but 0 is a root of f only if $B = 0$. Thus if $A = 0$, either f has all distinct roots, or $f = T^{n+2}$. Suppose now $A \neq 0$. If α is a multiple root, then

$$0 = f'(\alpha) = \alpha f'(\alpha) = (n+2)(\alpha)^{n+2} + A\alpha.$$

Thus

$$(\alpha)^{n+2} = -A\alpha/(n+2),$$

and so α, also being a root of f, satisfies

$$(1 - 1/(n+2))A\alpha + B = 0,$$

i.e., we have $\alpha = -((n+2)/(n+1))B/A$. If $\alpha = 0$, then $B = 0$, in which case our polynomial is $T^{n+2} + AT$ with $A \neq 0$, which has $n+2$ distinct roots. If $\alpha \neq 0$, then α is not a root of $f'' = (n+2)(n+)T^n$. So in this $\alpha \neq 0$ case, f has at most one multiple root, and that multiple root occurs with multiplicity two. □

Suppose now that $p = 2$, and that $n+3$ is odd. To show that $Z(n,3)$ has at most isolated singularities, it suffices to show that its intersection with the hypersurface $s_{n+2}(a_1, ..., a_{n+3}) = 0$, call it $W(n,3)$ is a nonsingular curve.

Lemma 2.4. *If $p = 2$, and $n+3$ is odd, then $W(n,3)$ is a nonsingular curve.*

Proof. We have homogeneous coordinates $a_1, ..., a_{n+3}$, and $W(n,3)$ is defined by the $n+1$ equations

$$s_i(a_1, ..., a_{n+3}) = 0,\ 1 \leq i \leq n, \text{ together with } s_{n+2}(a_1, ..., a_{n+3}) = 0.$$

We know that $W(n,3)$ is a complete intersection of dimension one (because imposing two more equations, $s_{n+1} = 0$ and $s_{n+3} = 0$, gives the empty scheme). To analyze its singular locus, we use the following variant of Tarleton's lemma.

Lemma 2.5. *Suppose $n+3 \geq 5$ is odd. Then the determinant of the $(n+1) \times (n+1)$ Jacobian matrix*

$$(\partial s_i/\partial a_j)_{i=1,2,...,n,n+2,\ j=1,2,...,n+1}$$

in which the functions are $s_1, ..., s_n$ and s_{n+2}, and we differentiate with respect to $n+1$ of the $n+3$ variables $a_1, ..., a_{n+3}$, here with respect to $a_1, ..., a_{n+1}$, is

$$\pm(a_{n+2} + a_{n+3}) \prod_{1 \leq i < j \leq n+1} (a_i - a_j).$$

Proof. Exactly as in the proof of the Tarleton formula, the determinant visibly vanishes if $a_i = a_j$ for some pair $1 \leq i < j \leq n+1$. Let us admit temporarily that the determinant also vanishes if $a_{n+2} + a_{n+3} = 0$. Then the determinant is divisible by its asserted value, and both sides of of the asserted identity are homogeneous of the same degree. So the determinant must be some integer multiple of its asserted value. It that integer multiple were not ± 1, the determinant would vanish identically in some finite characteristic p. In that characteristic, the affine surface defined by the same equations, $s_1 = ... = s_n = s_{n+2} = 0$

in $\mathbb{A}^{n+3}$ would be everywhere singular, and hence the scheme defined by further specializing $s_{n+1} = A, s_{n+3} = B$ would be everywhere singular, for any choices of A and B in any algebraically closed field K of the bad characteristic p. If $p = 2$, or more generally if p does not divide $n + 3$, take $A = 0$, $B = 1$.Then we are looking at the K-scheme of complete factorizations of $1 + T^{n+3}$ over a field K in which $n + 3$ is invertible; this K-scheme is finite étale. If p is odd and p divides $n+3$, take $A = B = 1$. Then we are looking at the K-scheme of complete factorizations of $1 + T^{n+1} + T^{n+3}$ over a field K in which $n + 3 = 0$. Equivalently, passing to the palindromic polynomial, we are looking at the K-scheme of complete factorizations of $f(T) := 1+T^2+T^{n+3}$ over a field K of odd characteristic p in which $n + 3 = 0$. This polynomial has all distinct roots (the only root of its derivative $f'(T) = 2T$ is 0, which is not a root of f), so the K-scheme of its complete factorizations is again finite étale over K.

It remains to show that $(a_{n+2}+a_{n+3})$ divides the determinant. Recall that

$$\partial s_i/\partial a_j = s_{i-1}(\text{all variables except } a_j).$$

It will be important to specify exactly which variables are involved. Thus for $j = 1, 2, ..., n + 1$, we will write

$$\mathbb{S}_i(\text{not } a_j) := s_i(\text{all variables } a_1, ..., a_{n+3} \text{ except } a_j),$$

$$S_i(\text{not } a_j) := s_i(\text{all variables } a_1, ..., a_{n+1} \text{ except } a_j).$$

One checks easily that, **modulo** the relation $a_{n+2} + a_{n+3} = 0$, for each $i \geq 2$ we have

$$\mathbb{S}_i(\text{not } a_j) = S_i(\text{not } a_j) + a_{n+2}a_{n+3}S_{i-2}(\text{not } a_j).$$

[Think of $\mathbb{S}_i(\text{not } a_j)$ as a sum of monomials. The terms in which neither a_{n+2} nor a_{n+3} occurs give precisely $S_i(\text{not } a_j)$. The terms in which both a_{n+2} and a_{n+3} occur give $a_{n+2}a_{n+3}S_{i-2}(\text{not } a_j)$. The terms in which exactly one of $\{a_{n+2}, a_{n+3}\}$ occurs cancel identically, modulo the relation $a_{n+2} + a_{n+3} = 0$.]

Notice now that the lowest row of our Jacobian matrix has entries the $\mathbb{S}_{n+1}(\text{not } a_j)$. Because there are only $n+3$ variables in total, in the identity (modulo the relation $a_{n+2} + a_{n+3} = 0$)

$$\mathbb{S}_{n+1}(\text{not } a_j) = S_{n+1}(\text{not } a_j) + a_{n+2}a_{n+3}S_{n-1}(\text{not } a_j),$$

the term $S_{n+1}(\text{not } a_j)$ vanishes identically. Thus (modulo the relation $a_{n+2} + a_{n+3} = 0$) we have

$$\mathbb{S}_{n+1}(\text{not } a_j) = a_{n+2}a_{n+3}S_{n-1}(\text{not } a_j),$$

$$\mathbb{S}_{n-1}(\text{not } a_j) = S_{n-1}(\text{not } a_j) + a_{n+2}a_{n+3}S_{n-3}(\text{not } a_j),$$

...,

$$\mathbb{S}_3(\text{not } a_j) = S_3(\text{not } a_j) + a_{n+2}a_{n+3}S_1(\text{not } a_j).$$

Again modulo the relation $a_{n+2} + a_{n+3} = 0$, we have

$$S_1(\text{not } a_j) = \mathbb{S}_1(\text{not } a_j).$$

So for each index $1 \leq j \leq n+1$ we get the relation

$$\mathbb{S}_{n+1}(\text{not } a_j) = -\sum_{i=1}^{n/2}(-a_{n+2}a_{n+3})^i\mathbb{S}_{n+1-2i}(\text{not } a_j.)$$

This relation shows that (modulo the relation $a_{n+2} + a_{n+3} = 0$) the bottom row of the Jacobian matrix is a $\mathbb{Z}[a_{n+2}a_{n+3}]$-linear combination of the rows above it. Thus modulo the relation $a_{n+2} + a_{n+3} = 0$, the determinant vanishes. □

It remains to show that if n is even and k has characteristic $p = 2$, then $W(n, 3)$ is smooth. In view of the determinant formula of the previous lemma, it suffices to show that for any algebraically closed overfield K of k, and for any two elements $A, B \in K$ other than $0, 0$, the polynomial $f(T) := T^{n+3} + AT^2 + B$ has at least $n + 2$ distinct roots. If $A = 0$, then B is nonzero, and our polynomial has $n + 3$ distinct roots. If A is nonzero, then the derivative $f'(T) = 2AT$ has only $T = 0$ as a root, and this is also a root of f only when $B = 0$. In this last case, f is $T^{n+3} + AT^2$, which has $n + 2$ distinct roots, 0 being the unique double root; we then number the roots so that one but not both of a_{n+2}, a_{n+3} is this double root 0 to get a nonzero minor. This concludes the proof of Lemma 2.4. □

This concludes the proof of Lemma 2.1. □

Lemma 2.6. *Let k be a field of characteristic p. We have the following results about the scheme $X(n, d, \vec{b})/k$.*

(1) *$X(n, d, \vec{b})$ is a complete intersection of dimension d.*
(2) *If $d = 2$ and p does not divide $(n + 2)(n + 1)$, $X(n, 2, \vec{b})$ is a complete intersection surface with at most isolated singularities.*
(1) *If $p = 2, d = 3$ and n is even, $X(n, 3, \vec{b})$ is a complete intersection threefold with a singular locus of dimension ≤ 1.*

Proof. If we intersect with the hyperplane $z = 0$, we get $Z(n, d)/k$, which is a complete intersection of dimension $d-1$. Hence $X(n, d, \vec{b})/k$ is a complete intersection of dimension d. In the situations of (2) and (3), the singular locus has dimension at most $d - 2$, otherwise its intersection with $z = 0$ would have dimension $\geq d - 2$. But this

intersection lies in the singular locus of $Z(n,d)$, and we invoke Lemma 2.1. □

Lemma 2.7. *Let k be a finite field, $X \subset \mathbb{P}^{n+d}/k$ a projective complete intersection of dimension $d \geq 0$ and multidegree $(1,2,...,n)$. Then we have the following results.*

(1) *For any prime ℓ invertible in k, the sum of the $\mathbb{Q}_\ell$-Betti numbers of $X_{\overline{k}}$ is bounded by*
$$C(n,d) := 9 \times 2^n (3+n^2)^{n+d+1}.$$

(2) *With $q := \#k$ we have the estimate*
$$\#X(k) \leq C(n,d) q^d.$$

(3) *If $d \geq 1$ and the dimension of the singular locus is at most $d-2$, then with $q := \#k$, we have the estimate*
$$|\#X(k) - q^d| \leq C(n,d) q^{d-1/2}.$$

Proof. The estimate for the sum of the Betti numbers is given in [Ka-SB, Cor. of Thm. 3, second inequality]. The "trivial" estimate (2) results from the Lefschetz trace formula, the vanishing of $H^i(X_{\overline{k}}, \mathbb{Q}_\ell)$ for $i > 2d$, and the deep fact [De-Weil II, 3.3.1] that H^i is mixed of weight $\leq i$. The estimate (3) for a complete intersection whose singular locus has codimension two or more is [Ka-HooleyApp, proof of Thm. 1], where it is shown that $H^{2d}(X_{\overline{k}}, \mathbb{Q}_\ell) = \mathbb{Q}_\ell(-d)$, the one-dimensional $\mathbb{Q}_\ell$ vector space on which $Frob_k$ acts as q^d. A more elementary way of seeing this is to remark that a complete intersection is Cohen-Macauley [Eis, Prop.18.13, Section 18.15]. If it is of dimension $d \geq 1$, it is geometrically connected (Lefschetz hyperplane theorem for H^0). If its singular locus has codimension ≥ 2, then it is normal (Serre's criterion, cf. [A-K, VII 2.14]). Being normal and geometrically connected, it is geometrically irreducible, and hence its H^{2d} is as asserted. □

With these preliminaries out of the way, we can now prove Theorem 1.1. Suppose first the p does not divide $(n+2)(n+1)$. Given a finite field k and a vector $\vec{b} \in k^{n+2}$, we must show that if $q := \#k$ is (explicitly) sufficiently large, then
$$U(n,2,\vec{b})(k) := X(n,2,\vec{b})(k) \setminus Z(n,2)(k)$$
is nonempty. First apply part (2) of Lemmas 2.1 and 2.6, then Lemma 2.7 to both $X(n,2,\vec{b})$ and $Z(n,2)$, to get
$$|\#X(n,2,\vec{b})(k) - q^2| \leq C(n,2) q^{3/2},$$
$$|\#Z(n,2)(k)| \leq C(n,1) q.$$

So we have

$$\#U(n,2,\vec{b})(k) \geq q^2 - C(n,2)q^{3/2} - C(n,1)q.$$

So $U(n,2,\vec{b})(k)$ will certainly be nonempty provided

$$\sqrt{q} \geq C(n,2) + C(n,1).$$

So the asserted constant $C_2(n)$ of Theorem 1.1 may be taken to be

$$C_2(n) := (C(n,2) + C(n,1))^2.$$

Suppose now that k has characteristic $p = 2$ and n is even. Using now part (3) of Lemmas 2.1 and 2.6, together with Lemma 2.7, we get

$$|\#X(n,3,\vec{b})(k) - q^3| \leq C(n,3)q^{5/2},$$

$$|\#Z(n,3)(k)| \leq C(n,2)q^2.$$

So we have

$$\#U(n,3,\vec{b})(k) \geq q^3 - C(n,3)q^{5/2} - C(n,2)q^2.$$

So $U(n,3,\vec{b})(k)$ will certainly be nonempty provided

$$\sqrt{q} \geq C(n,3) + C(n,2).$$

So the asserted constant $C_3(n)$ of Theorem 1.1 may be taken to be

$$C_3(n) := (C(n,3) + C(n,2))^2.$$

3. Supplementary results

If we are willing to increase the constant $C_2(n)$, respectively the constant $C_3(n)$, of Theorem 1.1, we can further impose that in representing a given element as a product of $n+2$, respectively $n+3$, elements $1 + a_i X$, all the a_i are nonzero and $a_i \neq a_j$ for $i \neq j$. Here are the formal statements.

Theorem 3.1. *Given an integer $n \geq 1$, denote by $D_2(n)$ the constant*

$$D_2(n) := (C(n,2) + (1 + (n+2)^2)C(n,1))^2,$$

and by $D_3(n)$ the constant

$$D_3(n) := (C(n,3) + (1 + (n+3)^2)C(n,2))^2.$$

Then we have the following results.

(1) *For any finite field k with $\#k \geq D_2(n)$ whose characteristic p does not divide $(n+2)(n+1)$, any element of $BigWitt_n(k)$ can be written as the product of $n+2$ elements $1 + a_i X$, with all the a_i nonzero and $a_i \neq a_j$ for $i \neq j$.*

(2) *If n is even, then for any finite field k with $\#k \geq D_3(n)$ of characteristic $p = 2$, any element of $BigWitt_n(k)$ can be written as the product of $n+3$ elements $1+a_iX$, with all the a_i nonzero and $a_i \neq a_j$ for $i \neq j$.*

Proof. (1)Fix two indices $i \neq j$. The subvariety of $X(n, 2, \vec{b})$ defined by the two equations $a_i = 0$ and $a_i = a_j$ is itself the complete intersection $X(n, 0, \vec{b})$ of dimension 0. Therefore imposing either of these two equations alone defines a complete intersection of dimension 1, which may be seen as a complete intersection in $\mathbb{P}^{n+1}$ of multidegree $(1, 2, ..., n)$. So the sum of its $\mathbb{Q}_\ell$- Betti numbers, for any ℓ invertible in k, is bounded by $C(n, 1)$. So we have the trivial estimate that, putting $q := \#k$, each such variety has at most $C(n, 1)q$ k-valued points. Inverting $z(\prod_i a_i)(\prod_{i<j}(a_i - a_j))$ amounts to removing $1 + n + 2 + (n + 2)(n + 1) = 1 + (n + 2)^2$ such varieties, thus removing at most

$$(1 + (n + 2)^2)C(n, 1))q$$

points from $X(n, 2, \vec{b})(k)$, which has at least $q^2 - C(n, 2)q^{3/2}$ points.

To prove (2), we essentially repeat this argument. The subvariety of $X(n, 3, \vec{b})$ defined by the vanishing of either of the equations $a_i = 0$ or $a_i = a_j$ is a complete intersection of dimension 2, which may be seen as a complete intersection in $\mathbb{P}^{n+2}$ of multidegree $(1, 2, ..., n)$, so has at most $C(n, 2)q^2$ k-valued points. Inverting $z(\prod_i a_i)(\prod_{i<j}(a_i - a_j))$ amounts to removing $1 + n + 3 + (n + 3)(n + 2) = 1 + (n + 3)^2$ such varieties, while $X(n, 3, \vec{b})(k)$ has at least $q^3 - C(n, 3)q^{5/2}$ points. □

The advantage of this last result is that it generalizes to complete noetherian local rings.

Theorem 3.2. *Fix an integer $n \geq 1$. Let A be a complete notherian local ring whose residue field k is finite and has characteristic p. Then we have the following results.*

(1) *If p does not divide $(n + 2)(n + 1)$ and if $\#k \geq D_2(n)$, any element of $BigWitt_n(A)$ can be written as the product of $n + 2$ elements $1 + a_iX$, with all the a_i and all the differences $a_i - a_j$, $i \neq j$, invertible in A.*

(2) *If n is even, $p = 2$ and $\#k \geq D_3(n)$, any element of $BigWitt_n(A)$ can be written as the product of $n + 3$ elements $1 + a_iX$, with all the a_i and all the differences $a_i - a_j$, $i \neq j$, invertible in A.*

Proof. (1)Given an element $v = 1 + \sum_{i=1}^n b_iX^i \in BigWitt_n(A)$, denote by $\overline{v} = 1 + \sum_{i=1}^n \overline{b_i}X^i \in BigWitt_n(k)$ its reduction modulo the maximal

ideal of A. By Theorem 3.1, we can write $\overline{v}$ as the product of $n+2$ distinct elements $1+\alpha_i X$, with $\alpha_i \in k^\times$. Multiplying out the product of these elements $1+\alpha_i X$, we get a polynomial of degree $n+2$,

$$\prod_{i=1}^{n+2}(1+\alpha_i X) = 1 + \sum_{i=1}^{2n+1} \beta_i X^i$$

in which β_{n+2} is invertible and in which we have

$$\beta_i = \overline{b_i}$$

for $1 \leq i \leq n$. For each integer j in $[n+1, n+2]$, choose a lift $b_j \in A$ of β_j. Then the polynomial

$$1 + \sum_{i=1}^{n+2} b_i X^i \in A[X],$$

reduced modulo the maximal ideal of A, has $n+2$ distinct (reciprocal) roots $\alpha_i \in k^\times$. Apply Hensel's lemma to obtain unique lifts $a_i \in A^\times$ of $\alpha_i \in k^\times$ with

$$1 + \sum_{i=1}^{n+2} b_i X^i = \prod_{i=1}^{n+2}(1+a_i X).$$

Reducing mod X^{n+1} gives the desired expression for v.

The proof of (2) is identical, with $n+2$ replaced by $n+3$. □

4. The girth

What can we say about the girth of the graph $\mathcal{G}(n,k)$, for k a finite field? Recall the girth is the least integer $g \geq 1$ such that the unit element $1 \in BigWitt_n(k)$ can be written as the product of g elements $1+a_i X$ with all $a_i \in k^\times$. We must have $g \geq n+1$, otherwise we get an equation of too low degree for X. We can very well have $g = n+1$ in some cases.

Lemma 4.1. *Let k have characteristic p. Write $n+1$ as $n+1 = p^a m$ with m prime to p. If k contains all m of the m'th roots of unity, then $\mathcal{G}(n,k)$ has girth $n+1$.*

Proof. Indeed, we have $1 = (\prod_{\zeta \in \mu_m(k)}(1-\zeta X))^{p^a} \in BigWitt_n(k)$. □

We can very well have $g \geq n+2$ as well.

Lemma 4.2. *Let k have characteristic p. Suppose $q := \#k$ is such that $\gcd(p(q-1), n+1) = 1$. Then $\mathcal{G}(n,k)$ has girth $g \geq n+2$.*

Proof. If $q-1$ is relatively prime to $n+1$, then the map $t \mapsto t^{n+1}$ is bijective on $k^\times$. If we have an expression

$$1 = \prod_{i=1}^{n+1}(1 - a_i X) \in BigWitt_n(k), \text{ all } a_i \in k^\times$$

then we have an identity of polynomials

$$\prod_{i=1}^{n+1}(1 - a_i X) = 1 - CX^{n+1}$$

with $C \in k^\times$. We may write C uniquely as B^{n+1} with $B \in k^\times$. So this identity becomes

$$\prod_{i=1}^{n+1}(1 - a_i X) = 1 - B^{n+1}X^{n+1}.$$

Therefore each a_i is an $n+1$'st root of B^{n+1}, so by uniqueness each $a_i = B$. So our identity becomes

$$(1 - BX)^{n+1} = 1 - B^{n+1}X^{n+1}.$$

But $n+1$ is prime to p, so already the linear term of $(1-BX)^{n+1}$ is nonzero in k. □

These last two lemmas, together with Corollary 1.3, show that if, for example, $n+1$ is an odd prime ℓ, then as p varies, the graph $\mathcal{G}(n, \mathbb{F}_p)$ will have girth $n+1$ for all p which are 1 mod ℓ, and will have girth $n+2$ for all other large p.

5. Relation to Galois theory

The fact that $X(n, 2, \vec{b})/k$, and hence $U(n, 2, \vec{b})/k$, is geometrically irreducible when p does not divide $(n+2)(n+1)$ leads to another proof of Cohen's theorem [C, Thm. 1] that for K any field of characteristic p not dividing $(n+2)(n+1)$, and for any polynomial $f(T) \in K[T]$ of degree $n+2$, the polynomial $f(T) + AT + B$ with two indeterminate coefficients A, B has galois group the full symmetric group S_{n+2} over the field $K(A, B)$, cf. [Ka-FP, proof of Thm. 3] for a discussion of this sort of implication.

The situation in characteristic 2 is similar. When $p = 2$ and n is even, we have shown that $W(n, 3)$, the intersection of $Z(n, 3)$ with $s_{n+1} = 0$, is a complete intersection curve which is smooth. Therefore the intersection of $X(n, 3, \vec{b})/k$ with $s_{n+1} = 0$ is a complete intersection surface with at worst isolated singularities, so is geometrically irreducible. This geometrically irreducibility in turn leads to another proof of Cohen's

theorem [C-Corr., Thm. 2'] that for K any field of characteristic 2 and $f(T) \in K[T]$ of degree $n+3$, the polynomial $f(T) + AT^2 + B$ with two indeterminate coefficients A, B has galois group the full symmetric group S_{n+3} over the field $K(A, B)$. In fact, it was this result of Cohen that led us to the consideration of the variety $W(n, 3)$.

References

[A-K] Altman, A. and Kleiman, S., Introduction to Grothendieck Duality Theory, Springer, Lecture Notes in Mathematics 140, 1970.

[C] Cohen, S. D., The Galois group of a polynomial with two indeterminate coefficients. Pacific J. Math. 90 (1980), no. 1, 63-79.

[C-Corr.] Cohen, S. D., Corrections to: "The Galois group of a polynomial with two indeterminate coefficients". Pacific J. Math. 97 (1981), no. 2, 483-486.

[C-Graph] Cohen, S. D., Polynomial factorisation and an application to regular directed graphs. Finite Fields Appl. 4 (1998), 316346..

[De-Weil II] Deligne, P., La conjecture de Weil II. Publ. Math. IHES 52 (1981), 313-428.

[Eis] Eisenbud, D., Commutative Algebra with a view toward Algebraic Geometry, Springer, GTM 150, 1995.

[Ka-FP] Katz, N., Factoring polynomials in finite fields: an application of Lang-Weil to a problem in graph theory. Math. Ann. 286 (1990), no. 4, 625-637.

[Ka-HooleyApp] Katz, N., Appendix:Number of points on singular complete intersections. Appendix to Hooley, C., On the number of points on a complete intersection over a finite field. J. Number Theory 38 (1991), no. 3, 338-358.

[Ka-MG] Katz, N., On the monodromy groups attached to certain families of exponential sums. Duke Math. J. 54 (1987), no. 1, 41-56.

[Ka-SB] Katz, N., Sums of Betti numbers in arbitrary characteristic, Finite Fields Appl. 7 (2001), no. 1, 29-44.

[La-Pr] Lascoux, Alain; Pragacz, Piotr, Jacobians of symmetric polynomials. Ann. Comb. 6 (2002), no. 2, 169-172.

[Muir-III] Muir, T., The theory of Determinants in the historical order of development, Vol. III, The period 1861 to 1880, MacMillan and Co., Limited, 1920.

[Sc] Scott, R.F., On some alternating functions of n variables, Messenger of Math. 11 (1882) 98-103.

[T] Tarleton, F.A., Question 2367, Educ. Times, xix. p. 280; Math. from Educ. Times IX, pp. 69-70.

Princeton University, Mathematics, Fine Hall, NJ 08544-1000, USA
E-mail address: nmk@math.princeton.edu