

GROWTH OF THE IDEAL GENERATED BY A QUADRATIC BOOLEAN FUNCTION

JINTAI DING, TIMOTHY HODGES, VICTORIA KRUGLOV

ABSTRACT. We give exact formulas for the growth of the ideal $A\lambda$ for λ a quadratic element of the algebra of Boolean functions over the Galois field $GF(2)$. That is, we calculate $\dim A_k\lambda$ where A_k is the subspace of elements of degree less than or equal to k . These results clarify some of the assertions made in the article of Yang and Chen [YC] concerning the efficiency of the XL algorithm in cryptography.

1. INTRODUCTION

The solution of polynomial equations has been a central question in mathematics since earliest times. Recently this problem has become a central topic in cryptography, in the form of the solution of multivariate polynomial equations over a finite field. For instance, in multivariate public key cryptography [DGS] the public key is given by a set of polynomials

$$P(x_1, \dots, x_n) = (P_1(x_1, \dots, x_n), \dots, P_m(x_1, \dots, x_n))$$

over a finite field. To encrypt a message (x'_1, \dots, x'_n) , one computes the value

$$(y'_1, \dots, y'_m) = P(x'_1, \dots, x'_n) = (P_1(x'_1, \dots, x'_n), \dots, P_m(x'_1, \dots, x'_n)).$$

In order to attack this cipher directly, one needs to solve the system of equations

$$(y'_1, \dots, y'_m) = P(x_1, \dots, x_n).$$

Similarly, the algebraic attack [CP, AK] on symmetric cryptosystems transforms the problem into one of solving systems of polynomial equations. For instance in the case of AES, this attack produces a system of 6000 sparse equations in approximately 1600 variables. Thus understanding the complexity of solving multivariate equations is a critical problem which has not only theoretical significance but also serious practical implications.

The two main types of algorithm used to solve such systems of equations are the Groebner basis algorithm family including the F4 and F5 variants [Bu, F1, F2]; and the XL algorithms including FXL and mutant XL [CKPS, DBMMW]. The most commonly quoted estimates of the computational complexity use formulas developed recently in [YC, BFSY], which were originally intended for the XL algorithms only. The key idea of the XL algorithm, as applied to the solution of a system of m quadratic equations $f_i(\mathbf{x}) = \mathbf{0}$, is to successively eliminate variables by finding

This work grew out of discussions in the Taft Research Seminar on post-quantum cryptography presented at the University of Cincinnati by Bo-Yin Yang. The authors thank Yang for many interesting conversations on this topic. They also thank the Taft Research Center at the University of Cincinnati for its support of the seminar.

1-variables polynomials inside the ideal generated by the $f_i(\mathbf{x})$. Specifically, one applies an elimination process to the space of functions spanned by the $\mathbf{x}^{\mathbf{b}} f_i(\mathbf{x})$ where $\mathbf{x}^{\mathbf{b}}$ is a monomial of total degree less than or equal to a fixed number D . The key to understanding the complexity of the algorithm is to understand the dimension of this subspace. Yang and Chen produced estimates of the complexity of the XL algorithm based on formulas for these dimensions. Although the complexity formulas were widely used and were in close agreement with experimental evidence, a number of authors have noted that the proofs of the dimension theorems are based on unreliable heuristic arguments.

Because of the significance of these complexity formulas and their implications in cryptography, we believe that it is important to systematically study this question and to lay a solid mathematical foundation for future developments in this area. In this paper, we begin with the simplest case, that of a single quadratic polynomial over the field $GF(2)$.

Of course, over a field of characteristic zero the question is totally trivial. The complication when dealing with finite fields is that we are working not in the polynomial ring itself, but in the ring of the functions; that is, the polynomial ring reduced by the related field equations,

$$X_i^q - X_i = 0,$$

where q is the size of the field. This makes our question a highly complicated and non-trivial mathematical problem, as the reader will see from the results of this paper.

2. BASICS

Let F denote the Galois field $GF(2)$. Let $R = F[X_1, \dots, X_n]$ be the field of polynomials over F and let

$$A = F[X_1, \dots, X_n]/(X_1^2 + X_1, \dots, X_n^2 + X_n)$$

be the ring of Boolean functions.

Let $R_{(d)}$ be the space of homogeneous polynomials of degree d , so that $R = \bigoplus R_{(d)}$ is the usual grading. Let $R_d = \sum_{i=1}^d R_{(i)}$ be the set of polynomials of degree less than or equal to d , so that

$$F = R_0 \subset R_1 \subset \dots \subset R$$

is the usual filtration by degree. Denote by $\pi : R \rightarrow A$ the usual projection and let $A_{(i)} = \pi(R_{(i)})$ and let $A_i = \pi(R_i)$. Then $A = \bigoplus A_{(d)}$ is a vector space direct sum but not a gradation of rings, but $A_0 \subset A_1 \subset \dots \subset A_n = A$ is a ring filtration. One may define a concept of degree for an element $\lambda \in A$ by saying that $\deg \lambda = \min\{d \mid \lambda \in A_d\}$. We say that element is quadratic if it has degree two.

We calculate explicitly $\dim A_k \lambda$ for a quadratic element $\lambda \in A$. we first need to introduce some of the notation needed to describe this number. Set

$$\sigma(n, k) = \sum_{j=0}^k \binom{n}{j} \quad \delta(n, k) = \sum_{i=0}^{\lfloor k/2 \rfloor} (-1)^i \sigma(n, k - 2i),$$

The main theorem of [YC] asserts that $\dim A_k \lambda \leq \delta(n, k)$ for all k and that equality holds when “a) $\lambda - a$ is not factorizable for any $a \in F$; and b) λ contains enough degree two monomials to make $\deg \lambda m = \deg m + 2$ for all monomials m ”. As was pointed out in [D], the argument contains some major gaps and it is easy to find

examples that show that the statement is not true in general. In fact we shall see that there are no quadratic $\lambda \in A$ for which the statement is true. However, it turns out that formula claimed by Yang and Chen is true for values of k that are small relative to the rank of λ . For larger k , a small additional term is needed, but the value of $\delta(n, k)$ proves to be a reasonably close estimate for $\dim A_k \lambda$.

3. EQUIVALENCE, RANK AND TYPE

The dimension of $A_k \lambda$ is not the same for all quadratic elements λ . However it is obviously invariant under any automorphism that preserves degree. Inside the group of all automorphisms of A we have the subgroup of automorphisms that preserve degree; that is, the subgroup of all automorphisms ϕ such that $\phi(A_1) = A_1$. These are the *affine automorphisms*. We say that two elements of $\lambda, \lambda' \in A$ are equivalent if there exist an affine automorphism ϕ such that $\phi(\lambda) = \lambda'$.

Definition 3.1. Let $\lambda \in A$. We define the *rank* of λ to be the smallest positive integer r such that λ lies in a subalgebra generated by r linear elements. That is the smallest r such that there exists $l_1, \dots, l_r \in A_1$ with $\lambda \in F[l_1, \dots, l_r]$.

It is clear that the rank of an element is invariant under an affine automorphism. In general the set of elements of a given rank and degree is a union of a number of different equivalence classes. For quadratic elements there are two equivalence classes for even rank and one for odd rank.

Theorem 3.2. *Let $\lambda \in A$ be a quadratic element of rank r .*

- (1) *If r is even, then λ is either equivalent to $x_1 x_2 + \dots x_{r-1} x_r$ or $x_1 x_2 + \dots x_{r-1} x_r + 1$. Moreover these two elements are not equivalent.*
- (2) *If r is odd, then λ is equivalent to $x_1 x_2 + \dots x_{r-2} x_{r-1} + x_r$.*

Proof. This follows from the classification of quadratic elements in the polynomial ring given in [LN]. □

Thus it suffices to calculate $\dim A_k \lambda$ for the elements listed in the theorem. we begin with the maximal rank case which is the simplest.

4. EVEN MAXIMAL RANK

The calculation of $\dim A_k \lambda$ in [YC] uses the exact sequence:

$$0 \longrightarrow A_k \cap A(\lambda + 1) \longrightarrow A_k \longrightarrow A_k \lambda \longrightarrow 0$$

In order to apply induction we would like $A_k \cap A(\lambda + 1) = A_{k-2}(\lambda + 1)$. While this often holds, it is not always true. For instance, note that, for r even,

$$(x_1 + 1)(x_3 + 1) \dots (x_{r-1} + 1)(x_1 x_2 + \dots x_{r-1} x_r) = 0$$

so that $(x_1 + 1)(x_3 + 1) \dots (x_{r-1} + 1) \in A_{r/2} \cap \text{Ann}(x_1 x_2 + \dots x_{r-1} x_r) = A_{r/2} \cap A(x_1 x_2 + \dots x_{r-1} x_r + 1)$ but $(x_1 + 1)(x_3 + 1) \dots (x_{r-1} + 1) \notin A_{r/2-2}(x_1 x_2 + \dots x_{r-1} x_r + 1)$. It turns out that these elements are the principal obstructions to the above equality when $r = n$.

Theorem 4.1. *Suppose that n is even and suppose that $\lambda = x_1 x_2 + \dots x_{n-1} x_n$. Then*

- (1) $A_k \cap A(\lambda + 1) = A_{k-2}(\lambda + 1)$ for all $k < n/2$ and $k \geq n/2 + 2$
- (2) $A_k \cap A \lambda = A_{k-2} \lambda$ for all k .

Proof. (1) It is clear that $A_{k-2}(\lambda + 1) \subseteq A_k \cap A(\lambda + 1)$. Using induction on n , we prove that $A_k \cap A(\lambda + 1) \subseteq A_{k-2}(\lambda + 1)$ for $2 \leq k < n/2$ and $k \geq n/2 + 2$

Consider the case when $n = 2$ and $\lambda = x_1x_2$. Let $a \in A$, so that $a = a_0 + a_1x_1 + a_2x_2 + a_3x_1x_2$, for some $a_i \in F$. Then

$$a(\lambda + 1) = a_0 + a_1x_1 + a_2x_2 + (a_0 + a_1 + a_2)x_1x_2$$

From this it is clear that $A_0 \cap A(\lambda + 1) = 0$ and that $A(\lambda + 1) = A_1(\lambda + 1)$. Hence the result is clearly true in the case $n = 2$.

Now let $A' = F[x_3, x_4, \dots, x_m]$ and $\lambda' = x_3x_4 + \dots + x_{n-1}x_n$ and assume the assertion true for λ' and A' . Note that A is a free A' -module with basis $\{1, x_1, x_2, x_1x_2\}$. Thus an arbitrary element of A is of the form $a = a'_0 + a'_1x_1 + a'_2x_2 + a'_3x_1x_2$, where $a'_i \in A'$. Since $x_1x_2 = \lambda + \lambda'$ and $\lambda(\lambda + 1) = 0$ we see that $x_1x_2(\lambda + 1) = \lambda'(\lambda + 1)$ and so $a(\lambda + 1) = \tilde{a}(\lambda + 1)$ where $\tilde{a} = (a'_0 + a'_3\lambda') + a'_1x_1 + a'_2x_2$. Hence an arbitrary element of $A(\lambda + 1)$ is of the form $a(\lambda + 1)$ where $a = a'_0 + a'_1x_1 + a'_2x_2$ for some $a'_i \in A'$. Suppose that $a(\lambda + 1) \in A_k$. Now

$$\begin{aligned} a(\lambda + 1) &= (a'_0 + a'_1x_1 + a'_2x_2)(x_1x_2 + \lambda' + 1) \\ &= a'_0(\lambda' + 1) + a'_1(\lambda' + 1)x_1 + a'_2(\lambda' + 1)x_2 + (a'_0 + a'_1 + a'_2)x_1x_2. \end{aligned}$$

Because of the linear independence of the elements $\{1, x_1, x_2, x_1x_2\}$ over A' each of the summands must also lie in A_k . Hence $a'_0(\lambda' + 1) \in A_k$; $a'_1(\lambda' + 1), a'_2(\lambda' + 1) \in A_{k-1}$ and $a'_0 + a'_1 + a'_2 \in A'_{k-2}$.

Suppose that $k < n/2$. Then $k - 1 < n/2 - 1 = (n - 2)/2$. Hence by induction, $A'_{k-1} \cap A'(\lambda' + 1) = A'_{k-3}(\lambda' + 1)$. So there exist $b'_1, b'_2 \in A'_{k-3}$, such that $a'_1(\lambda' + 1) = b'_1(\lambda' + 1)$ and $a'_2(\lambda' + 1) = b'_2(\lambda' + 1)$. Let $b'_0 = a'_0 + a'_1 + a'_2 + b'_1 + b'_2$. Then $b'_0 \in A'_{k-2}$ since $a'_0 + a'_1 + a'_2 \in A'_{k-2}$ and $b'_1 + b'_2 \in A'_{k-3}$. Moreover $b'_0(\lambda' + 1) = a'_0(\lambda' + 1)$. Now define $b = b'_0 + b'_1x_1 + b'_2x_2$. Then, $b \in A_{k-2}$ and

$$\begin{aligned} b(\lambda + 1) &= b'_0(\lambda' + 1) + b'_1(\lambda' + 1)x_1 + b'_2(\lambda' + 1)x_2 + (b'_0 + b'_1 + b'_2)x_1x_2 \\ &= a'_0(\lambda' + 1) + a'_1(\lambda' + 1)x_1 + a'_2(\lambda' + 1)x_2 + (a'_0 + a'_1 + a'_2)x_1x_2. \\ &= a(\lambda + 1) \end{aligned}$$

Thus $A_k \cap A(\lambda + 1) \subseteq A_{k-2}(\lambda + 1)$ as required.

If $k \geq n/2 + 2$, then $k - 1 \geq n/2 - 1 = (n - 2)/2$ and the same argument proves the second part of the assertion.

A similar argument proves the part (2) of the theorem. \square

Before proving our dimension theorem, we assemble some results that we shall be using.

Lemma 4.2. *Let n be even and let $\lambda = x_1x_2 + x_3x_4 + \dots + x_{n-1}x_n$. Then,*

$$\dim A\lambda = 2^{n-1} - 2^{\frac{n}{2}-1} \quad \text{and} \quad \dim A(\lambda + 1) = 2^{n-1} + 2^{\frac{n}{2}-1}.$$

Proof. See [LN, Theorem 6.32]. \square

Lemma 4.3.

$$\begin{aligned} \sum_{i=0}^{\lfloor n/4 \rfloor} \binom{n}{4i} &= \frac{1}{2} \left(2^{n-1} + 2^{n/2} \cos \frac{n\pi}{4} \right) \\ \sum_{i=0}^{\lfloor (n-1)/4 \rfloor} \binom{n}{4i+1} &= \frac{1}{2} \left(2^{n-1} + 2^{n/2} \sin \frac{n\pi}{4} \right) \end{aligned}$$

$$\sum_{i=0}^{\lfloor (n-2)/4 \rfloor} \binom{n}{4i+2} = \frac{1}{2} \left(2^{n-1} - 2^{n/2} \cos \frac{n\pi}{4} \right)$$

$$\sum_{i=0}^{\lfloor (n-3)/4 \rfloor} \binom{n}{4i+3} = \frac{1}{2} \left(2^{n-1} - 2^{n/2} \sin \frac{n\pi}{4} \right)$$

Proof. See [GR, 0.153]. □

Define

$$\epsilon(k) = \cos \left(\frac{k\pi}{2} \right) + \sin \left(\frac{k\pi}{2} \right)$$

Lemma 4.4. *For any positive integer n ,*

- (1) $\delta(n, n) = 2^{n-1} + \epsilon(n/2) 2^{\frac{n}{2}-1}$
- (2) $\delta(n, n-1) = 2^{n-1} + \epsilon(n/2-1) 2^{\frac{n}{2}-1}$

Proof. For part (1) observe that

$$\begin{aligned} \delta(n, n) &= \sum_{i=0}^{\lfloor n/4 \rfloor} \binom{n}{n-4i} + \sum_{i=0}^{\lfloor (n-1)/4 \rfloor} \binom{n}{n-1-4i} \\ &= \sum_{i=0}^{\lfloor n/4 \rfloor} \binom{n}{4i} + \sum_{i=0}^{\lfloor (n-1)/4 \rfloor} \binom{n}{4i+1} \\ &= 2^{n-1} + \left[\cos \frac{n\pi}{4} + \sin \frac{n\pi}{4} \right] 2^{n/2} \\ &= 2^{n-1} + \epsilon(n/2) 2^{n/2} \end{aligned}$$

Similarly for part (2),

$$\begin{aligned} \delta(n, n-1) &= \sum_{i=0}^{\lfloor (n-1)/4 \rfloor} \binom{n}{n-1-4i} + \sum_{i=0}^{\lfloor (n-2)/4 \rfloor} \binom{n}{n-2-4i} \\ &= \sum_{i=0}^{\lfloor (n-1)/4 \rfloor} \binom{n}{4i+1} + \sum_{i=0}^{\lfloor (n-2)/4 \rfloor} \binom{n}{4i+2} \\ &= 2^{n-1} + \left[\sin \frac{n\pi}{4} - \cos \frac{n\pi}{4} \right] 2^{n/2} \\ &= 2^{n-1} + \left[\cos \frac{(n-2)\pi}{4} + \sin \frac{(n-2)\pi}{4} \right] 2^{n/2} \\ &= 2^{n-1} + \epsilon(n/2-1) 2^{n/2} \end{aligned}$$

□

Theorem 4.5. *Suppose that n is even and let $\lambda = x_1 x_2 + \dots + x_{n-1} x_n$. Then*

$$\dim A_k \lambda = \begin{cases} \delta(n, k), & \text{if } k < n/2 \\ \delta(n, k) - (\epsilon(k - n/2) + 1) 2^{\frac{n}{2}-1}, & \text{if } n/2 \leq k \leq n \end{cases}$$

$$\dim A_k (\lambda + 1) = \begin{cases} \delta(n, k), & \text{if } k < n/2 + 2 \\ \delta(n, k) - (\epsilon(k - n/2) - 1) 2^{\frac{n}{2}-1}, & \text{if } n/2 \leq k \leq n \end{cases}$$

Proof. We first prove the assertion that $\dim A_k \lambda = \delta(n, k) = \dim A_k(\lambda + 1)$ for $k < n/2$. We need two base cases, $k = 0$ and $k = 1$. When $k = 0$, $A_k = F$, and so it is clear that $\dim A_0 \lambda = \dim A_0(\lambda + 1) = 1 = \delta(n, 1)$. When $k = 1$ and $n > 2$, the maps from A_1 to $A_1 \lambda$ and $A_1(\lambda + 1)$ are both bijective by Theorem 4.1. So $\dim A_1 \lambda = \dim A_1(\lambda + 1) = \dim A_1 = \sigma(n, 1) = \delta(n, 1)$.

Now suppose $1 < k < n/2$. Since $\text{Ann } \lambda = A(\lambda + 1)$ and $A_k \cap (\lambda + 1) = A_{k-2}(\lambda + 1)$ we have the exact sequence

$$0 \longrightarrow A_{k-2}(\lambda + 1) \longrightarrow A_k \longrightarrow A_k \lambda \longrightarrow 0$$

Applying the inductive hypothesis yields $\dim A_k \lambda = \dim A_k - \dim A_{k-2}(\lambda + 1) = \sigma(n, k) - \delta(n, k - 2) = \delta(n, k)$, as desired. A similar argument works for $A_k(\lambda + 1)$.

We now prove that for $n/2 \leq k \leq n$, $\dim A_k \lambda = \delta(n, k) - (\epsilon(k - n/2) + 1)2^{\frac{n}{2}-1}$ and $\dim A_k(\lambda + 1) = \delta(n, k) - (\epsilon(k - n/2) - 1)2^{\frac{n}{2}-1}$ by reverse induction using $k = n$ and $k = n - 1$ as base cases. Consider the case $k = n$. Since $A_n = A$, $\dim A_n \lambda = 2^{n-1} - 2^{\frac{n}{2}-1} = \delta(n, n) - \epsilon(n/2)2^{n/2} - 2^{\frac{n}{2}-1} = \delta(n, n) - (\epsilon(n/2) + 1)2^{\frac{n}{2}-1}$, as required. Similarly, $\dim A_n(\lambda + 1) = 2^{n-1} + 2^{\frac{n}{2}-1} = \delta(n, n) - \epsilon(n/2)2^{n/2} + 2^{\frac{n}{2}-1} = \delta(n, n) - (\epsilon(n/2) - 1)2^{\frac{n}{2}-1}$.

Now consider the case $k = n - 1$. Observe that $A_{n-1} \lambda \supset A_{n-2} \lambda = A_n \cap A \lambda = A \lambda$. So $\dim A_{n-1} \lambda = \dim A_n \lambda$. However, using Lemma 4.4 we have that

$$\begin{aligned} & \delta(n, n - 1) - (\epsilon(n - 1 - n/2) + 1)2^{\frac{n}{2}-1} \\ &= (2^{n-1} + \epsilon(n/2 - 1)2^{\frac{n}{2}-1}) - (\epsilon(n/2 - 1) + 1)2^{\frac{n}{2}-1} \\ &= 2^{n-1} - 2^{\frac{n}{2}-1} = \dim A \lambda \end{aligned}$$

A similar argument proves that $A_{n-1}(\lambda + 1) = A(\lambda + 1)$ and that the formula holds in this case also.

We now assume the formula holds for $k + 2$ and prove that it holds for k , provided that $k \geq n/2 + 2$. Again we have the short exact sequence

$$0 \longrightarrow A_k \lambda \longrightarrow A_{k+2} \longrightarrow A_{k+2}(\lambda + 1) \longrightarrow 0$$

So that

$$\begin{aligned} \dim A_k \lambda &= \dim A_{k+2} - \dim A_{k+2}(\lambda + 1) \\ &= \sigma(n, k + 2) - (\delta(n, k + 2) - (\epsilon(k + 2 - n/2) - 1)2^{\frac{n}{2}-1}) \\ &= \delta(n, k) - (\epsilon(k - n/2) + 1)2^{\frac{n}{2}-1} \end{aligned}$$

since $\epsilon(k + 2) = -\epsilon(k)$. Similarly the exact sequence

$$0 \longrightarrow A_k(\lambda + 1) \longrightarrow A_{k+2} \longrightarrow A_{k+2} \lambda \longrightarrow 0$$

yields

$$\begin{aligned} \dim A_k(\lambda + 1) &= \dim A_{k+2} - \dim A_{k+2} \lambda \\ &= \sigma(n, k + 2) - (\delta(n, k + 2) - (\epsilon(k + 2 - n/2) + 1)2^{\frac{n}{2}-1}) \\ &= \delta(n, k) - \epsilon(k - n/2) - 1)2^{\frac{n}{2}-1} \end{aligned}$$

as required.

It remains to deal with the cases when $k = n/2$ and $k = n/2 + 1$. Using the argument from the upward induction we get in these cases that

$$\dim A_k(\lambda + 1) = \dim A_k - \dim A_k(\lambda) = \delta(n, k) = \delta(n, k) - \epsilon(k - n/2) - 1)2^{\frac{n}{2}-1}$$

since $\epsilon(0) = \epsilon(1) = 1$. The downward induction argument above extends to show that $\dim A_k(\lambda) = \dim A_{k+2} - \dim A_{k+2}(\lambda + 1) = \delta(n, k) - (\epsilon(k - n/2) + 1)2^{\frac{n}{2}-1}$ in these cases. \square

5. ODD MAXIMAL RANK CASE

If n is odd and λ is quadratic of rank $4n$, then as observed above, $\lambda \sim x_1x_2 + \dots x_{n-2}x_{n-1} + x_n$.

Theorem 5.1. *Suppose that n is odd let $\lambda = x_1x_2 + \dots x_{n-2}x_{n-1} + x_n$. Then*

$$A_k \cap A\lambda = A_{k-2}\lambda$$

for $k \neq (n+1)/2$.

Proof. The proof is very similar to the proof of Theorem 4.1. Again, it is clear that $A_{k-2}\lambda \subseteq A_k \cap A\lambda$. Using induction on n , we prove that $A_k \cap A\lambda \subseteq A_{k-2}\lambda$ for $k \neq (n+1)/2$

Consider the case when $n = 3$ and $\lambda = x_1x_2 + x_3$. It is easily verified by hand that $A_1 \cap A\lambda = \{0\}$ and that $A\lambda = A_1\lambda$ so that $A_3 \cap A\lambda = A_1\lambda$.

Now suppose that $n \geq 5$. Let $A' = F[x_3, x_4, \dots, x_n]$ and $\lambda' = x_3x_4 + \dots + x_{n-2}x_{n-1} + x_n$ and assume the assertion true for λ' and A' . As above, note that A is a free A' -module with basis $\{1, x_1, x_2, x_1x_2\}$. Again an arbitrary element of $A\lambda$ is of the form $a\lambda$ where $a = a'_0 + a'_1x_1 + a'_2x_2$ for some $a'_i \in A'$.

Let $a\lambda \in A_k$ where a is as above. Now

$$\begin{aligned} a\lambda &= (a'_0 + a'_1x_1 + a'_2x_2)(x_1x_2 + \lambda') \\ &= a'_0\lambda' + a'_1\lambda'x_1 + a'_2\lambda'x_2 + (a'_0 + a'_1 + a'_2)x_1x_2. \end{aligned}$$

Because of the linear independence of the elements $\{1, x_1, x_2, x_1x_2\}$ over A' each of the summands must also lie in A_k . Hence $a'_0\lambda' \in A_k$; $a'_1\lambda', a'_2\lambda' \in A_{k-1}$ and $a'_0 + a'_1 + a'_2 \in A'_{k-2}$.

Suppose that $k \neq (n+1)/2$. Then $k-1 \neq ((n-2)+1)/2$. Hence by induction, $A'_{k-1} \cap A'\lambda' = A'_{k-3}\lambda'$. So there exist $b'_1, b'_2 \in A'_{k-3}$, such that $a'_1\lambda' = b'_1\lambda'$ and $a'_2\lambda' = b'_2\lambda'$. Let $b'_0 = a'_0 + a'_1 + a'_2 + b'_1 + b'_2$. Then $b'_0 \in A'_{k-2}$ since $a'_0 + a'_1 + a'_2 \in A'_{k-2}$ and $b'_1 + b'_2 \in A'_{k-3}$. Moreover $b'_0\lambda' = a'_0\lambda'$. Now define $b = b'_0 + b'_1x_1 + b'_2x_2$. Then, $b \in A_{k-2}$ and

$$\begin{aligned} b\lambda &= b'_0\lambda' + b'_1\lambda'x_1 + b'_2\lambda'x_2 + (b'_0 + b'_1 + b'_2)x_1x_2 \\ &= a'_0\lambda' + a'_1\lambda'x_1 + a'_2\lambda'x_2 + (a'_0 + a'_1 + a'_2)x_1x_2. \\ &= a\lambda \end{aligned}$$

Thus $A_k \cap A\lambda \subseteq A_{k-2}\lambda$ as required. \square

Theorem 5.2. *Suppose that n is odd and let $\lambda = x_1x_2 + \dots x_{n-2}x_{n-1} + x_n$. Then*

$$\dim A_k\lambda = \begin{cases} \delta(n, k), & \text{if } k < (n+1)/2 \\ \delta(n, k) - \epsilon(k - n/2)2^{\frac{n}{2}-1}, & \text{if } k \geq (n+1)/2 \end{cases}$$

Proof. Since all quadratic elements of A of maximal rank are affine equivalent, the assertion of the theorem is equivalent to the assertion that the result holds for all such elements. In order for the induction to work correctly (that is, to include both the cases of $\dim A_k\lambda$ and $\dim A_k(\lambda + 1)$), we need to work in the framework of this

more general assertion. The proof that $\dim A_k \lambda = \delta(n, k)$ if $k < (n+1)/2$ proceeds exactly as for Theorem 4.5 using Theorem 5.1 in place of Theorem 4.1.

It remains to prove that for $(n+1)/2 \leq k \leq n$, $\dim A_k \lambda = \delta(n, k) - \epsilon(k - n/2)2^{\frac{n}{2}-1}$. We again prove the result by reverse induction using $k = n$ and $k = n-1$ as base cases. For the case $k = n$, note first that by the symmetry of λ and $\lambda + 1$, $\dim A_n \lambda = 2^{n/2}$. Moreover,

$$\delta(n, k) - \epsilon(k - n/2)2^{\frac{n}{2}-1} = \delta(n, n) - \epsilon(n/2)2^{\frac{n}{2}-1} = 2^{n/2}$$

by Lemma 4.4. Now consider the case $k = n-1$ and assume that $n > 3$. Observe that $A_{n-1} \lambda = A_{n+1} \cap A \lambda = A \lambda$. So $\dim A_{n-1} \lambda = \dim A_n \lambda$. On the other hand, using Lemma 4.4 we have that

$$\begin{aligned} \delta(n, n-1) - \epsilon(n-1 - n/2)2^{\frac{n}{2}-1} \\ &= (2^{n-1} + \epsilon(n/2 - 1)2^{\frac{n}{2}-1}) - \epsilon(n/2 - 1)2^{\frac{n}{2}-1} \\ &= 2^{n-1} = \dim A \lambda \end{aligned}$$

So the result holds in this case also.

We now assume the formula holds for $k+2$ and prove that it holds for k , provided that $(n+1)/2 < k < n-2$. The short exact sequence

$$0 \longrightarrow A_k \lambda \longrightarrow A_{k+2} \longrightarrow A_{k+2}(\lambda + 1) \longrightarrow 0$$

implies that

$$\begin{aligned} \dim A_k \lambda &= \dim A_{k+2} - \dim A_{k+2}(\lambda + 1) \\ &= \sigma(n, k+2) - (\delta(n, k+2) - \epsilon(k+2 - n/2)2^{\frac{n}{2}-1}) \\ &= \delta(n, k) - \epsilon(k - n/2)2^{\frac{n}{2}-1} \end{aligned}$$

since $\epsilon(k+2) = -\epsilon(k)$. □

6. GENERAL CASE

Now consider a quadratic element $\lambda \in A$ of arbitrary rank $r \leq n$. Without loss of generality we assume that $\lambda \in A' = F[x_1, \dots, x_r]$ and that λ has one of the three canonical forms with respect to the variables x_1, \dots, x_r . The dimension of $A_k \lambda$ can be computed from the dimensions of the $A'_k \lambda$. Recall that we make the convention that $A_j = 0$ for $j < 0$,

Theorem 6.1.

$$\dim A_k \lambda = \sum_{i=0}^{n-r} \binom{n-r}{i} \dim A'_{k-i} \lambda$$

Proof. Let $S = \{x_{r+1}, \dots, x_n\}$, let \mathcal{P} be the power set of S and define x_S to be the product of the $x_i \in S$. Then the x_S clearly form a basis for A as a free A' -module. Let V_j be the span of the elements x_S of degree j . Then $A_k = \bigoplus_{i=0}^{n-r} A'_{k-i} V_i$ and hence $\dim A_k \lambda = \sum_{i=0}^{n-r} \dim A'_{k-i} V_i \lambda = \sum_{i=0}^{n-r} \binom{n-r}{i} \dim A'_{k-i} \lambda$. □

Corollary 6.2. *If $k < \text{rank } \lambda$, then $\dim A_k \lambda = \delta(n, k)$.*

Proof. This follows from the identity $\delta(n, k) = \sum_{i=0}^{n-r} \binom{n-r}{i} \delta(r, k-i)$ which itself follows from the analogous Vandermonde identity for binomial coefficients. □

Corollary 6.3. *Let λ be a quadratic element of rank r , then*

$$|\dim A_k \lambda - \delta(n, k)| \leq 2^{n-\frac{r}{2}}$$

7. CONCLUSION

Our results here simultaneously validate and refute the assertions made in [YC]. On the one hand they provide strong evidence that the results may be true in some generality when k is small relative to the rank of the polynomials, a case which is highly significant from the point of applications to cryptography and in particular to the analysis of the XL algorithm. On the other hand they show that no simple formula can hold for all k for any fixed λ .

The rationale for this work was to provide a detailed study of the specific case of a single quadratic polynomial over $GF(2)$ in order to better inform conjectures in the general case. Based on these results we draw the following conclusions.

- It is unlikely that it will be possible to calculate exact values for $\dim A_k \lambda$ similar to those given in Theorem 4.5 and Theorem 5.2 for λ of higher degree except in some special cases, due to the exponentially increasing number of affine equivalence classes in higher degree.
- It is likely that the important Corollary 6.2 will generalize to the case of arbitrary finite fields and higher degree polynomials.
- Similarly it may be possible to calculate reasonable bounds on $\dim A_k \lambda$ similar to those in Corollary 6.3 in these more general cases.

At this stage the most interesting problem is to determine the validity of Yang and Chen's assertions for sets of quadratic polynomials. Corollary 6.2 gives hope that the formula will be true for small k under some reasonable assumptions of "generic position". We hope to return to this question in a subsequent paper.

REFERENCES

- [AK] Frederik Armknecht and Matthias Krause, *Algebraic Attacks on Combiners with Memory*, Crypto 2003, August 17-21, Santa Barbara, CA, USA, LNCS V. 2729, 2003, Springer
- [BFSY] M. Bardet, J.-C. Faugère, B. Salvy and B.-Y. Yang, *Asymptotic Expansion of the Degree of Regularity for Semi-Regular Systems of Equations*, MEGA 2005 Sardinia (Italy) ,
- [DBMMW] Johannes Buchmann, Mohamed Saied Emam Mohamed, Wael Said Abdel Mageed Mohamed and Ralf-Philipp Weinmann, *Mutant XL*, First International Conference on Symbolic Computation and Cryptography – SCC 2008
- [Bu] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Innsbruck, 1965
- [CKPS] Nicolas T. Courtois, Alexander Klimov, Jacques Patarin and Adi Shamir, *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations*, Eurocrypt2000, LNCS, page392–407, Springer
- [CP] Nicolas T. Courtois and Josef Pieprzyk, *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations*, Asiacrypt 2002, Springer 267–287
- [D] C. Diem, *The XL-Algorithm and a Conjecture from Commutative Algebra*, Advances in cryptology - ASIACRYPT 2004, 323–337, Lecture Notes in Comput. Sci., 3329, Springer, Berlin, 2004.
- [DGS] Jintai Ding, Jason Gower and Dieter Schmidt, *Multivariate Public-Key Cryptosystems*, Advances in Information Security, Springer, 2006, ISBN 0-387-32229-9
- [F1] Jean-Charles Faugère, *A new efficient algorithm for computing Gröbner bases (F_4)*, Pure App Alg, Volume 139, 1999, 61–88
- [F2] Jean-Charles Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5)*, ISSAC 2002, Pages 75–83
- [GR] S. Gradsteyn and I.M. Ryzhik, *Table of Integrals, Series, and Products, 7-th edition*, Academic Press, San Diego, 2007.
- [LN] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its applications, 20, Cambridge University Press, 1997.

- [YC] B.-Y. Yang and J.-M. Chen,, “Theoretical Analysis of XL over Small Fields,” Proc. 9th Australasian Conference on Info. Sec. and Privacy, volume 3108, Lecture Notes in Computer Science, pages 277-288, 2004.

E-mail address: `jintai.ding@uc.edu`, `timothy.hodges@uc.edu`

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF CINCINNATI, CINCINNATI, OH,
45221-0025 USA