Growth of the Ideal Generated by a Quadratic Boolean Function

Jintai Ding, Timothy J. Hodges, and Victoria Kruglov*

Department of Mathematical Sciences,
University of Cincinnati,
Cincinnati, OH, 45221-0025 USA
jintai.ding@uc.edu, timothy.hodges@uc.edu, kruglov@email.uc.edu

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, Chen and Courtois [22,23] concerning the efficiency of the XL algorithm.

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 [12], the public key is given by a set of polynomials

$$P(x_1, .., x_n) = (P_1(x_1, .., x_n), ..., P_m(x_1, .., x_n))$$

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

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

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

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

Similarly, the algebraic attack [10,3] on symmetric cryptosystems transforms the problem of attacking the cryptosystems 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. Though we know that in general solving a set of random nonlinear equations is a NP-complete problem,

* 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.

N. Sendrier (Ed.): PQCrypto 2010, LNCS 6061, pp. 13–27, 2010.

the understanding of the complexity of solving multivariate equations is still a critical problem which has not only theoretical significance but also serious practical implications.

In 2000, Courtois et al. introduced the XL algorithm [8] to solve such systems of equations. The 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 linear or 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. In [8,9], some heuristic complexity estimates were given for the XL algorithm, but these estimates have been shown to be incorrect [18].

The most commonly quoted estimates of the computational complexity of the XL algorithm use formulas developed in [22], and which were further explored in [24,23]. Yang and Chen produced estimates of the complexity of the XL algorithm based on formulas for the dimension of the space of functions spanned by the $\mathbf{x}^{\mathbf{b}} f_i(\mathbf{x})$. Although the complexity formulas were widely used (for instance, in [21,16,1,2,20,7]), and were in close agreement with experimental evidence, the proofs of the dimension theorems are based on unreliable heuristic arguments and are not correct. Some further exploration of these formulas was also recently done in [19], but based on some heuristic assumptions.

Another fundamental class of algorithms used to solve such systems of equations is the family of Gröbner basis algorithms including the F4 and F5 variants [6,13,14]. F4's implementation in Magma is considered the best in multivariate polynomial solving among all that are publicly available. We also know from [4] that F4 is actually a more efficient algorithm than the XL algorithm **if we assume** that both of them will solve the polynomials systems using Gaussian elimination to solve the systems of linear equations that arise. However, because of the sparse structure of the matrices associated to the XL algorithm, one can solve the linear systems more efficiently using the Wiedermann solver, which has advantages in terms of both speed and memory. It was demonstrated in the attack on the QUAD steam cipher [25] that the Wiedermann XL could indeed outperform the F4 algorithm. Therefore the complexity of the XL algorithm remains of great interests.

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 answer to the question is easy. 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 non-trivial mathematical problem, which turns out to have a surprisingly complex but elegant solution.

The complexity of the Gröbner basis algorithms F4 and F5 was analyzed in [5]. A few words of explanation are in order concerning the difficulty of our results compared to those in [5]. First, we consider here an arbitrary quadratic function, while the results in [5] concern the case of semi-regular sequences. Second we compute the exact dimension at each degree. The arguments in [5] concern the dimensions of the graded components of the ideal generated by the leading terms of the f_i in the associated graded ring (where $X_i^2 = 0$). While this enables one to pull back a certain amount of information to the original algebra of functions, it does not provide the exact dimensions that we calculate here.

2 The Yang-Chen Dimension Formulas

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

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

be the ring of Boolean functions.

Let $R_{(d)}$ be the space of homogeneous polynomials of degree d, so that $R = \oplus R_{(d)}$ is the usual grading. Let $R_d = \sum_{i=0}^{d} R_{(i)}$ be the set of polynomials of degree less than or equal to d, so that

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

is the usual filtration by degree. Denote by $\pi : R \to A$ the usual projection and let $A_{(i)} = \pi(R_{(i)})$ and let $A_i = \pi(R_i)$. Then $A = \oplus A_{(d)}$ is a vector space direct sum but not a gradation of rings, but $A_0 \subset A_1 \subset \cdots \subset A_n = A$ 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 an element is quadratic if it has degree two.

In this article we calculate explicitly $\dim A_k \lambda$ for a quadratic element $\lambda \in A$ and compare this result with that given by Yang and Chen in [22,23]. Let us briefly review the assertions in [23].

Let $\lambda_1, \ldots, \lambda_m \in A$ be a *semi-regular* [5] set of m quadratic elements. Corollary 4 of [23] asserts that

$$T - I = [t^D]\frac{(1+t)^n}{(1+t^2)^m(1-t)}$$

for all $D < D_{reg}$. Here $[t^D](1+t)^n(1+t^2)^{-m}(1-t)^{-1}$ denotes the coefficient of t^D in the powers series expansion of $(1+t)^n(1+t^2)^{-m}(1-t)^{-1}$; $T = \dim A_D$; $I = \dim \sum_i A_{D-2}\lambda_i$; and $D_{reg} = \min\{D \mid [t^D](1+t)^n(1+t^2)^{-m}(1-t)^{-1} \leq 0\}$.

This formula has the following explicit form when $m = 1$. Set

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

Then for $D < D_{reg}$,

$$T - I = [t^D] \frac{(1+t)^n}{(1+t^2)(1-t)} = \delta(n, D)$$

Since $T = \dim A_D = \sigma(n,D)$, this yields $I = \sigma(n,D) - \delta(n,D) = \delta(n, D-2)$. Hence

$$\dim A_{D-2}\lambda = \delta(n, D-2)$$

for any semi-regular quadratic element λ and for any $D < D_{reg}$. While this assertion is suggestive of the actual behavior, the statement of the result is not adequate to include any useful assertions when $m = 1$. It is easily verified that for the definition of D_{reg} given above and in [23], $D_{reg} = \infty$. As can be seen in Theorems 5.3 and 7.1, the assertion that $\dim A_{D-2}\lambda = \delta(n, D-2)$ for all D cannot hold for any λ (except for very small values of n). In fact, no λ can be semi-regular (again except for exceptional cases), so the theorem as stated in [23] is vacuous rather than false in the case $m = 1$. The appropriate formulation of this assertion is that $\dim A_{D-2}\lambda = \delta(n, D-2)$ whenever $D - 2 < \operatorname{rank} \lambda/2$, (Corollary 7.2). In [23], the authors also claim, that in the non-semi-regular case "the value I can only decrease". When $m = 1$, this becomes the assertion that $\dim A_{D-2}\lambda \leq \delta(n, i-2)$ for all $D \leq D_{reg}$. Theorem 5.3 shows that this claim is false.

3 Some Combinatorial Lemmas

Before getting into the details of the man results we present some elementary identities concerning $\sigma(n,k)$ and $\delta(n,k)$ that we will need later.

Lemma 3.1. *The following analogs of the Vandermonde identity hold for $\sigma(n,k)$ and $\delta(n,k)$:*

$$\sigma(n,k) = \sum_{i=0}^{k} \binom{n-r}{i} \sigma(r, k-i) \quad \delta(n,k) = \sum_{i=0}^{k} \binom{n-r}{i} \delta(r, k-i)$$

Proof. The Vandermonde identity for binomial coefficients states that

$$\binom{n}{k} = \sum_{i=0}^{k} \binom{n-r}{i} \binom{r}{k-i}.$$

Hence

$$\begin{aligned}\sum_{i=0}^{k}\binom{n-r}{i}\sigma(r,k-i) &= \sum_{i=0}^{k}\binom{n-r}{i}\sum_{j=0}^{k-i}\binom{r}{j}\\ &= \sum_{i=0}^{k}\sum_{j=0}^{k-i}\binom{n-r}{i}\binom{r}{k-i-j}\\ &= \sum_{j=0}^{k}\sum_{i=0}^{k-j}\binom{n-r}{i}\binom{r}{k-j-i}\\ &= \sum_{j=0}^{k}\binom{n}{k-j} = \sum_{j=0}^{k}\binom{n}{j}\\ &= \sigma(n,k)\end{aligned}$$

Similarly,

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

Lemma 3.2. *For any $0 \le k \le n$,*

$$\delta(n,k) = \sum_{i=0}^{\lfloor k/4\rfloor}\binom{n}{k-4i} + \sum_{i=0}^{\lfloor (k-1)/4\rfloor}\binom{n}{k-1-4i}.$$

In particular,

$$\delta(n,n) = \sum_{i=0}^{\lfloor n/4\rfloor}\binom{n}{n-4i} + \sum_{i=0}^{\lfloor (n-1)/4\rfloor}\binom{n}{n-1-4i}$$

and

$$\delta(n,n-1) = \sum_{i=0}^{\lfloor (n-1)/4\rfloor}\binom{n}{n-1-4i} + \sum_{i=0}^{\lfloor (n-2)/4\rfloor}\binom{n}{n-2-4i}$$

Proof.

$$\begin{aligned}
\delta(n,k) = & \sum_{i=0}^{\lfloor k/2 \rfloor} (-1)^i \sigma(n, k-2i) \\
&= \sigma(n,k) - \sigma(n,k-2) + \sigma(n,k-4) - \cdots \pm \sigma(n, k-2\lfloor k/2 \rfloor) \\
&= \binom{n}{k} + \binom{n}{k-1} + \binom{n}{k-4} + \binom{n}{k-5} + \binom{n}{k-8} + \binom{n}{k-9} + \cdots \\
&= \binom{n}{k} + \binom{n}{k-4} + \binom{n}{k-8} + \cdots + \binom{n}{k-1} + \binom{n}{k-5} + \ldots \\
&= \sum_{i=0}^{\lfloor k/4 \rfloor} \binom{n}{k-4i} + \sum_{i=0}^{\lfloor (k-1)/4 \rfloor} \binom{n}{k-1-4i}
\end{aligned}$$

Lemma 3.3.

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

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

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

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

Proof. See [15, 0.153].

Define

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

Lemma 3.4. *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),

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

4 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 4.1. *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 $\ell_1, \ldots, \ell_r \in A_1$ with $\lambda \in F[\ell_1, \ldots, \ell_r]$.*

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

1. *If r is even, then λ is either equivalent to $x_1x_2 + \cdots + x_{r-1}x_r$ or $x_1x_2 + \cdots + x_{r-1}x_r + 1$. Moreover these two elements are not equivalent.*
2. *If r is odd, then λ is equivalent to $x_1x_2 + \cdots + x_{r-2}x_{r-1} + x_r$.*

Proof. This follows from the classification of quadratic elements in the polynomial ring given in [17].

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.

5 Even Maximal Rank

The calculation of $\dim A_k\lambda$ in [22] uses the exact sequence:

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

where the map from A_k to $A_k\lambda$ is just multiplication by λ. The kernel of this map is the intersection of $\operatorname{Ann}\lambda = \{b \in A \mid b\lambda = 0\}$ (the annihilator of λ) with A_k. It is well-known and easily verified that $\operatorname{Ann}\lambda = A(\lambda+1)$, so the kernel is $A_k \cap A(\lambda+1)$, yielding the exact sequence above. The kernel $A_k \cap A(\lambda+1)$ clearly contains $A_{k-2}(\lambda+1)$. 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,

$$(x_1+1)(x_3+1)\dots(x_{r-1}+1)(x_1x_2+\cdots+x_{r-1}x_r) = 0$$

so that $(x_1+1)(x_3+1)\dots(x_{r-1}+1) \in A_{r/2} \cap \operatorname{Ann}(x_1x_2+\cdots+x_{r-1}x_r) = A_{r/2} \cap A(x_1x_2+\cdots+x_{r-1}x_r+1)$ but $(x_1+1)(x_3+1)\dots(x_{r-1}+1) \notin A_{r/2-2}(x_1x_2+\cdots+x_{r-1}x_r+1)$. It turns out that these elements are the principal obstructions to the above equality when $r = n$.

Theorem 5.1. *Suppose that n is an even positive integer and suppose that $\lambda = x_1x_2+\cdots+x_{n-1}x_n$. Then*

1. *$A_k \cap A(\lambda+1) = A_{k-2}(\lambda+1)$ for all $0 \le k < n/2$ and $n/2+2 \le k \le n+2$*
2. *$A_k \cap A\lambda = A_{k-2}\lambda$ for all $0 \le k \le n+2$.*

Proof. (1) It is clear that $A_{k-2}(\lambda+1) \subseteq A_k \cap A(\lambda+1)$. Thus it suffices to prove that $A_k \cap A(\lambda+1) \subseteq A_{k-2}(\lambda+1)$ for $0 \le k < n/2$ and $n/2+2 \le k \le n+2$. Note that the two extreme cases are easily seen to be true. Since $A = A_n = A_{n+2}$, $A_{n+2} \cap A(\lambda+1) = A \cap A(\lambda+1) = A(\lambda+1) = A_n(\lambda+1)$. On the other hand, $A_{-2} = 0$ and $A_0 = F$. Since $\lambda+1$ is not a unit (because $\lambda(\lambda+1) = 0$), $A_0 \cap A(\lambda+1) = F \cap A(\lambda+1) = 0 = A_{-2}(\lambda+1)$.

We proceed by induction on n. Consider the case when $n = 2$ and $\lambda = x_1x_2$. It remains to show that $A_3 \cap A(\lambda+1) = A_1(\lambda+1)$; that is, that $A(\lambda+1) = A_1(\lambda+1)$. It is easy to verify directly that $\{x_1x_2+1, x_1x_2+x_1, x_1x_2+x_2\}$ forms a basis for $A(\lambda+1)$ and that this basis is contained in $A_1(\lambda+1)$.

We now assume the result is true for $n-2$ variables and deduce that it is true for n variables. Now let $A' = F[x_3, x_4, \dots, x_n]$ and $\lambda' = x_3x_4+\cdots+x_{n-1}x_n$ and assume that the assertion is 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 $a = a_0' + a_1'x_1 + a_2'x_2 + a_3'x_1x_2$, 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 $\tilde{a} = (a_0' + a_3'\lambda') + a_1'x_1 + a_2'x_2$. Hence an arbitrary element of $A(\lambda+1)$ is of the form $a(\lambda+1)$ where $a = a_0' + a_1'x_1 + a_2'x_2$ for some $a_i' \in A'$. Suppose that $a(\lambda+1) \in A_k$. Now

$$\begin{aligned} a(\lambda+1) &= (a_0' + a_1'x_1 + a_2'x_2)(x_1x_2 + \lambda' + 1) \\ &= a_0'(\lambda'+1) + a_1'(\lambda'+1)x_1 + a_2'(\lambda'+1))x_2 + (a_0' + a_1' + a_2')x_1x_2. \end{aligned}$$

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 $1 \leq k < n/2$. Then $0 \leq k-1 < n/2 - 1 = (n-2)/2$. 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 $b = b_0' + b_1'x_1 + b_2'x_2$. Then, $b \in A_{k-2}$ and

$$\begin{aligned} b(\lambda+1) &= b_0'(\lambda'+1) + b_1'(\lambda'+1)x_1 + b_2'(\lambda'+1))x_2 + (b_0' + b_1' + b_2')x_1x_2 \\ &= a_0'(\lambda'+1) + a_1'(\lambda'+1)x_1 + a_2'(\lambda'+1))x_2 + (a_0' + a_1' + a_2')x_1x_2. \\ &= a(\lambda+1) \end{aligned}$$

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

If on the other hand $n/2 + 2 \leq k \leq n+1$, then $(n-2)/2 = n/2 - 1 \leq k - 1 \leq n = (n-2)/2 + 2$. Again we may apply the induction hypothesis to deduce that $A_{k-1}' \cap A'(\lambda'+1)) = A_{k-3}'(\lambda'+1)$. The argument of the previous paragraph can be repeated verbatim to deduce that there exists a $b \in A_{k-2}$ such that $b(\lambda+1) = a(\lambda+1)$. Thus $A_k \cap A(\lambda+1) \subseteq A_{k-2}(\lambda+1)$ if $n/2+2 \leq k \leq n+2$.

(2) A similar argument proves the second part of the theorem. We need to show that $A_k \cap A(\lambda) \subseteq A_{k-2}(\lambda)$ for $0 \leq k \leq n+2$. the cases $k = 0$ and $k = n+2$ are easy to see directly just as in part (1).

The key difference lies in the base case $n = 2$. Here $\lambda = x_1x_2$, so $x_1\lambda = \lambda$ and $x_2\lambda = \lambda$. So $A\lambda = A_0\lambda$. Thus $A_0 \cap A\lambda = 0 = A_{-2}\lambda = 0$, $A_1 \cap A\lambda = 0 = A_{-1}\lambda = 0$, $A_2 \cap A\lambda = A_0\lambda$, $A_3 \cap A\lambda = A_0\lambda = A_1\lambda$. Thus the result is true when $n = 2$.

We now assume the result is true for $n-2$ variables and deduce that it is true for n variables. Suppose that $a\lambda \in A_k$. Then $a = a_0' + a_1'x_1 + a_2'x_2 + a_3'x_1x_2$, where $a_i' \in A'$. Since $x_1x_2 + \lambda' = \lambda$, and $\lambda(\lambda+1) = 0$, we have that $x_1x_2\lambda = (\lambda'+1)\lambda$. hence $a\lambda = [a_0' + a_3(\lambda'+1)] + a_1'x_1 + a_2'x_2$. hence we may assume that a is of the form $a = a_0' + a_1'x_1 + a_2'x_2$. Thus

$$\begin{aligned} a\lambda &= (a_0' + a_1'x_1 + a_2'x_2)(x_1x_2 + \lambda') \\ &= a_0'\lambda' + a_1'\lambda'x_1 + a_2'\lambda')x_2 + (a_0' + a_1' + a_2')x_1x_2. \end{aligned}$$

We deduce that $a_0'(\lambda'+1) \in A_k$; $a_1'(\lambda'+1), a_2'(\lambda'+1) \in A_{k-1}$ and $a_0' + a_1' + a_2' \in A_{k-2}'$. We can then use the induction hypothesis and the argument above to deduce that there exists a $b \in A_{k-2}$ such that $a\lambda = b\lambda$. Hence $A_k \cap A\lambda = A_{k-2}\lambda$, as required.

Lemma 5.2. *Let n be even and let $\lambda = x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n$. Then,*

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

Proof. Let $\mathcal{Z}(\lambda)$ be the set of zeros of λ. Then $|\mathcal{Z}(\lambda)| = \dim A/A\lambda$. it is well-known that $|\mathcal{Z}(\lambda)| = 2^{n-1} + 2^{\frac{n}{2}-1}$, [17, Theorem 6.32]. Hence $\dim A\lambda = \dim A - |\mathcal{Z}(\lambda)| = 2^n - (2^{n-1} + 2^{\frac{n}{2}-1}) = 2^{n-1} - 2^{\frac{n}{2}-1}$. The second assertion follows from the fact that $|\mathcal{Z}(\lambda)| = 2^{n-1} - 2^{\frac{n}{2}-1}$.

Theorem 5.3. *Suppose that n is even and let $\lambda = x_1x_2 + \cdots + x_{n-1}x_n$. Then*

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

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

Proof. We first prove the assertion that $\dim A_k\lambda = \delta(n,k) = \dim A_k(\lambda+1)$ for $0 \le k < n/2$ by induction on k. 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 5.1. 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 $\operatorname{Ann}\lambda = A(\lambda+1)$ 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 $n/2 \le k \le n$, $\dim A_k\lambda = \delta(n,k) - (\epsilon(k-n/2)+1)2^{\frac{n}{2}-1}$ 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 3.4 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 $k \ge n/2+2$. 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.

Note that the values of $\epsilon(k-n/2)+1$ form a sequence of the form $0, 0, 2, 2, 0, 0, 2, \ldots$ and those of $\epsilon(k-n/2)-1$ form the sequence $0, 0, -2, -2, 0, 0, -2, \ldots$. Thus in the first case, when $k > \operatorname{rank}\lambda/2$, the dimension of $A_k\lambda$ varies at or below $\delta(n,k)$, whereas in the second case it varies at or above $\delta(n,k)$. It is asserted in [22,23] that $\dim A_k\lambda \le \delta(n,k)$ whenever $k-2$ is less than the degree of regularity. This theorem shows that this assertion is false. In fact it is clear from this result that no such universal inequality is likely to hold in general.

6 Odd Maximal Rank

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

Theorem 6.1. *Suppose that n is odd let $\lambda = x_1x_2 + \cdots + x_{n-2}x_{n-1} + x_n$. 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 5.1. 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 $n \ge 5$. Let $A' = F[x_3, x_4, \ldots, x_n]$ and $\lambda' = x_3x_4 + \cdots + x_{n-2}x_{n-1} + x_n$ 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.

Theorem 6.2. *Suppose that n is odd and let $\lambda = x_1x_2 + \cdots + x_{n-2}x_{n-1} + x_n$. 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 5.3 using Theorem 6.1 in place of Theorem 5.1.

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 3.4. 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 3.4 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 $\epsilon(k+2) = -\epsilon(k)$.

7 General Case

Now consider a quadratic element $\lambda \in A$ of arbitrary rank $r \le n$. Without loss of generality we assume that $\lambda \in A' = F[x_1,\ldots,x_r]$ and that λ has one of the three canonical forms with respect to the variables $x_1,\ldots,x_r$. 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 7.1

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

Proof Let $S = \{x_{r+1},\ldots,x_n\}$, let $\mathcal{P}$ be the power set of S. For $T \in \mathcal{P}$ set $x_T = \prod_{i\in T} x_i$. Then the monomials x_T form a basis for A as a free A'-module. Let V_j be the span of the monomials x_T of degree j. Then $A_k = \oplus_{i=0}^{n-r} A'_{k-i}V_i$ and $A_k = \oplus_{i=0}^{k} A'_{k-i}\lambda V_i$ and hence $\dim A_k\lambda = \sum_{i=0}^{k} \dim A'_{k-i}\lambda V_i = \sum_{i=0}^{k} \binom{n-r}{i} \dim A'_{k-i}\lambda$.

Corollary 7.2. *If* $k < \operatorname{rank}\lambda/2$*, then* $\dim A_k\lambda = \delta(n,k)$.

Proof. From Theorem 7.1 we have that $\dim A_k\lambda = \sum_{i=0}^{k} \binom{n-r}{i} \dim A'_{k-i}\lambda$. Since $k-i \le k < \operatorname{rank}\lambda$ by hypothesis, we can conclude using Theorem 5.3 or Theorem 6.2 that $\dim A'_{k-i}\lambda = \delta(r,k-i)$. Hence

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

by Lemma 3.1.

Corollary 7.3. *Let* λ *be a quadratic element of rank* r*, then*

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

Proof. From Theorem 7.1 and Theorems 5.3 and 6.2 we have that

$$\begin{aligned}
|\dim A_k\lambda - \delta(n,k)| &= \left|\sum_{i=0}^{k}\binom{n-r}{i}\dim A'_{k-i}\lambda - \delta(n,k)\right| \\
&\le \left|\sum_{i=0}^{k}\binom{n-r}{i}\left(\delta(r,k-i)+2^{\frac{r}{2}}\right) - \delta(n,k)\right| \\
&= \left|\delta(n,k) + \sum_{i=0}^{k}\binom{n-r}{i}\left(2^{\frac{r}{2}}\right) - \delta(n,k)\right| \\
&\le 2^{n-r}2^{\frac{r}{2}} = 2^{n-\frac{r}{2}}
\end{aligned}$$

8 Conclusion

Our results give insight on the validity of [23, Corollary 4]. In particular we show that the formula $\dim A_k\lambda = \delta(n,k)$ is true for any λ provided that k is less than $(\operatorname{rank}\lambda)/2$. Furthermore, we see that the key conditions for the formula to hold involve both the rank and the equivalence class of the element λ. We proved that for large values of k, the value of $\dim A_k$ will oscillate above or below $\delta(n,k)$, depending on the equivalence type of λ. Thus no inequality of the form $\dim A_k\lambda \ge \delta(n,k)$ or $\dim A_k\lambda \le \delta(n,k)$ can hold universally.

References

1. Afzal, M., Masood, A.: Algebraic Cryptanalysis of A NLFSR Based Stream Cipher. In: The 3 rd International Conference on Information and Communication Technologies: From Theory to Applications, ICTTA 2008 (2008)
2. Albrecht, M., Cid, C.: Algebraic Techniques in Differential Cryptanalysis. In: Dunkelman, O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 193–208. Springer, Heidelberg (2009)
3. Armknecht, F., Krause, M.: Algebraic Attacks on Combiners with Memory. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 162–175. Springer, Heidelberg (2003)
4. Ars, G., Faugre, J.C., Imai, H., Kawazoe, M., Sugita, M.: Comparison Between XL and Grobner Basis Algorithms. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 338–353. Springer, Heidelberg (2004)
5. Bardet, M., Faugère, J.-C., Salvy, B., Yang, B.-Y.: Asymptotic Expansion of the Degree of Regularity for Semi-Regular Systems of Equations. In: MEGA 2005, Sardinia, Italy (2005)
6. Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, University of Innsbruck, PhD thesis (1965)
7. Cid, C., Leurent, G.: An Analysis of the XSL Algorithm. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 333–352. Springer, Heidelberg (2005)

8. Courtois, N.T., Klimov, A.B., Patarin, J., Shamir, A.: Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 392–407. Springer, Heidelberg (2000)
9. Courtois, N., Patarin, J.: About the XL Algorithm over GF(2). In: Joye, M. (ed.) CT-RSA 2003. LNCS, vol. 2612, pp. 141–157. Springer, Heidelberg (2003)
10. Courtois, N.T., Pieprzyk, J.: Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 267–287. Springer, Heidelberg (2002)
11. Diem, C.: The XL-Algorithm and a Conjecture from Commutative Algebra. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 323–337. Springer, Heidelberg (2004)
12. Ding, J., Gower, J., Schmidt, D.: Multivariate Public-Key Cryptosystems. In: Advances in Information Security. Springer, Heidelberg (2006) ISBN 0-387-32229-9
13. Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases (F_4). J. Pure Appl. Algebra 139(1-3), 61–88 (1999)
14. Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, pp. 75–83. ACM, New York (2002) (electronic)
15. Gradsteyn, S., Ryzhik, I.M.: Table of Integrals, Series, and Products, 7th edn. Academic Press, San Diego (2007)
16. Hu, Y.-H., Chou, C.-Y., Wang, L.-C., Lai, F.: Cryptanalysis of Variants of UOV. In: Katsikas, S.K., López, J., Backes, M., Gritzalis, S., Preneel, B. (eds.) ISC 2006. LNCS, vol. 4176, pp. 161–170. Springer, Heidelberg (2006)
17. Lidl, R., Niederreiter, H.: Finite Fields. In: Encyclopedia of Mathematics and its applications, p. 20. Cambridge University Press, Cambridge (1997)
18. Moh, T.T.: On The Method of “XL” And Its Inefficiency to TTM, IACR eprint server (2001), http://eprint.iacr.org/2001/047
19. Rønjom, S., Raddum, H.: Number of Linearly Independent Equations Generated by XL. In: Golomb, S.W., Parker, M.G., Pott, A., Winterhof, A. (eds.) SETA 2008. LNCS, vol. 5203, pp. 239–251. Springer, Heidelberg (2008)
20. Semaev, I.: On solving sparse algebraic equations over finite fields. Journal of Designs, Codes and Cryptography 49(1-3), 47–60 (2008)
21. Wong, K.K.-H., Colbert, B., Batten, L., Al-Hinai, S.: Algebraic Attacks on Clock-Controlled Cascade Ciphers. In: Barua, R., Lange, T. (eds.) INDOCRYPT 2006. LNCS, vol. 4329, pp. 32–47. Springer, Heidelberg (2006)
22. Yang, B.-Y., Chen, J.-M.: Theoretical Analysis of XL over Small Fields. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) ACISP 2004. LNCS, vol. 3108, pp. 277–288. Springer, Heidelberg (2004)
23. Yang, B.-Y., Chen, J.-M., Courtois, N.: On Asymptotic Security Estimates in XL and Grobner Bases-Related Algebraic Cryptanalysis. In: López, J., Qing, S., Okamoto, E. (eds.) ICICS 2004. LNCS, vol. 3269, pp. 401–413. Springer, Heidelberg (2004)
24. Yang, B.-Y., Chen, J.-M.: All in the XL Family: Theory and Practice. In: Park, C.-s., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 67–86. Springer, Heidelberg (2005)
25. Yang, B.-Y., Chen, C.-H., Bernstein, D.J., Chen, J.-M.: Analysis of QUAD. In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 290–308. Springer, Heidelberg (2007)