Quantum Period Reconstruction of Binary Sequences

Florina Piroi and Arne Winterhof

Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences,
Altenberger Str. 69, A-4040 Linz, Austria
firstname.lastname@oeaw.ac.at

Abstract. We consider the problem of determining the period of a binary sequence. For sequences with small autocorrelation we prove the existence of a polynomial time quantum algorithm for the above problem based on an algorithm of Hales and Hallgren. We apply this result to several concrete examples for which the autocorrelation can be estimated using known bounds on character sums.

Keywords: Period finding, quantum algorithm, binary sequences, autocorrelation, finite fields.

1 Introduction

According to *Kerckhoff's principle*, the security of a cryptosystem shall not be based on keeping the encryption algorithm secret but solely on keeping the encryption key secret. The security of many cryptographic sequences is only based on a secret period. Investigating the vulnerability of the secret key is of great importance for their choice.

We focus on the most important case of binary sequences and consider the problem of recovering the period T of a periodic sequence $\mathcal{S} = (s_n)_{n\geq 0}$ over $\mathbb{F}_2 = \{0, 1\}$ using a quantum algorithm.

Since the mapping $n \mapsto s_n$, $0 \leq n < T$, is not bijective, T cannot be recovered by the well-known algorithm of Shor [9]. Here we show that a result of Hales and Hallgren [4] is quite adequate for our purpose if the given sequence $\mathcal{S}$ has a small autocorrelation, which is an essential feature of cryptographic sequences.

We apply our result to several concrete examples:

- Generalisations of *Legendre sequences*;
- Generalisations of *Sidelnikov sequences*;
- Generalisations of *trace sequences*;
- *Elliptic curve trace sequences.*

As far as the authors are aware of, no classical algorithms are known that tackle with the above problems. We remark, however, that most of the results of this paper can be generalised to nonbinary sequences, see [10].

The main mathematical result of this paper is given in the proof of Theorem 1 in Section 3 and states that if the autocorrelation of a binary sequence is small then its distance from any sequence of smaller period is large.

M. Fossorier et al. (Eds.): AAECC 2006, LNCS 3857, pp. 60–67, 2006.

2 Preliminary Results

2.1 Autocorrelation

We recall the definition of the autocorrelation of a periodic binary sequence.

Let $\mathcal{S} = (s_n)_{n\geq 0}$ be a sequence over $\mathbb{F}_2$ and let $T > 1$ be the period of $\mathcal{S}$. The *autocorrelation function* AC of the sequence $\mathcal{S}$ with respect to the shift t is defined by the following relation:

$$\mathrm{AC}(\mathcal{S}, t) = \frac{1}{T} \sum_{n=0}^{T-1} (-1)^{s_n + s_{n+t}}, \quad 1 \leq t < T.$$

We need the following simple lemma.

Lemma 1. *Let $\mathcal{S} = (s_n)_{n\geq 0}$ be a sequence over $\mathbb{F}_2$, T the period of $\mathcal{S}$, and let $B \geq 0$ be fixed, such that*

$$\max_{1\leq t<T} |\mathrm{AC}(\mathcal{S}, t)| \leq BT^{-1}.$$

For a given t, $1 \leq t < T$, we denote with N_t the cardinality of the set

$$\{s_n \mid s_n = s_{n+t}, \quad 0 \leq n < T\}.$$

Then, for any t, $1 \leq t < T$, we have

$$\left| N_t - \frac{T}{2} \right| \leq \frac{B}{2}.$$

Proof. We clearly have that

$$|2N_t - T| = T \cdot |\mathrm{AC}(\mathcal{S}, t)| \leq B,$$

and the result of the lemma follows immediately.

2.2 Quantum Period Finding Algorithm

Given two periodic sequences $\mathcal{S}^1 = (s_n^1)_{n\geq 0}$ and $\mathcal{S}^2 = (s_n^2)_{n\geq 0}$ with periods T and t, respectively, we denote by $D(\mathcal{S}^1, \mathcal{S}^2)$ the number of integers $n \in [0, Tt-1]$ with $s_n^1 \neq s_n^2$. The following result can be immediately obtained from [4–Theorem 2].

Lemma 2. *For any constant $c > 0$, there is a quantum algorithm which computes in polynomial time, with probability at least $3/4$, the period of any sequence $\mathcal{S}^1$ of period T satisfying*

$$D(\mathcal{S}^1, \mathcal{S}^2) \geq \frac{Tt}{(\log T)^c},$$

for any sequence $\mathcal{S}^2$ of period $t < T$.

3 Reconstruction of the Period

In this section we state and prove the main theorem of this paper. Given a periodic binary sequence, the theorem below gives a condition which, when fulfilled, ensures the existence of a quantum algorithm for the reconstruction of the binary sequence's period.

Theorem 1. *Let $\mathcal{S} = (s_n)_{n\geq 0}$ be a sequence over $\mathbb{F}_2$ and T the period of $\mathcal{S}$, for which*

$$\max_{1\leq t<T} |\mathrm{AC}(\mathcal{S}, t)| \leq 1 - \frac{4}{(\log T)^c}$$

for some $c > 0$. Then there exists a quantum algorithm which computes T in polynomial time, with exponentially small probability of failure.

Proof. Let $\mathcal{S}^1 = (s^1_n)_{n\geq 0}$ be a sequence of period $t < T$ and let $\mathcal{K}_t$ be the set

$$\{s_n \mid s_n = s^1_n \text{ and } s_{n+t} = s^1_{n+t}, \quad 0 \leq n \leq Tt - 1\}.$$

Considering the definition of $D(\mathcal{S}, \mathcal{S}^1)$ we know that

$$Tt - 2D(\mathcal{S}, \mathcal{S}^1) \leq |\mathcal{K}_t|.$$

Also, for each $n \in \mathcal{K}_t$ we can write $s_n = s^1_n = s^1_{n+t} = s_{n+t}$ and thus $s_n = s_{n+t}$. Using the result of Lemma 1 with the bound $B = T(1 - 4(\log T)^{-c})$, we get

$$|\mathcal{K}_t| \leq tN_t \leq \frac{tT}{2}\left(2 - \frac{4}{(\log T)^c}\right).$$

We have now the following sequence of inequalities

$$Tt - 2D(\mathcal{S}, \mathcal{S}^1) \leq |\mathcal{K}_t| \leq \frac{tT}{2}\left(2 - \frac{4}{(\log T)^c}\right).$$

From here, we arrive at

$$D(\mathcal{S}, \mathcal{S}^1) \geq \frac{Tt}{(\log T)^c}.$$

The result of the theorem follows, then, from the application of Lemma 2.

The above theorem ensures us that a quantum algorithm for computing the period of a binary sequence exists, provided that the maximum autocorrelation of the sequence is small enough. The concrete description of the actual quantum algorithm and a proof of its correctness are not in the scope of this paper. We direct the interested reader to consult [4].

4 Applications

In this section we give some examples how Theorem 1 can be used to give the existence of quantum algorithms for recovering the period of special families of binary sequences. For each sequence in the examples below we give a bound for the maximum autocorrelation of the given sequence and then the condition for the existence of the quantum algorithm. Each of the corollaries formulated below follow immediately from Theorem 1.

4.1 Legendre and Related Sequences

We recall that a *Legendre sequence* $\mathcal{L} = (l_n)_{n\geq 0}$ is defined by

$$l_n = \begin{cases} 1 \text{ if } \left(\frac{n}{p}\right) = -1, \\ 0 \text{ otherwise,} \end{cases} \qquad n \geq 0,$$

where p is an odd prime and $\left(\frac{\cdot}{p}\right)$ denotes the *Legendre symbol.*

Now, given an odd prime p and a polynomial $f(X)$ over $\mathbb{F}_p$, we define the *generalised Legendre sequence* $\mathcal{L} = (l_n)_{n\geq 0}$ *of period* p*, with the polynomial* $f(X)$ as follows:

$$l_n = \begin{cases} 1, \text{ if } \left(\frac{f(n)}{p}\right) = -1, \\ 0, \text{ otherwise,} \end{cases} \qquad n \geq 0.$$

The following lemma can be immediately proved using Weil's bound for multiplicative character sums; see [6–Theorem 5.41].

Lemma 3. *For a generalised Legendre sequence* $\mathcal{L}$ *with a polynomial* $f(X) \in \mathbb{F}_p[X]$ *and period* p *such that, for any* $1 \leq t < p$, $f(X)f(X+t)$ *is not a square we have*

$$\max_{1\leq t<p} |\mathrm{AC}(\mathcal{L}, t)| \leq (2\deg(f) - 1)p^{-1/2} + 2\deg(f)p^{-1}.$$

Proof. Note that

$$(-1)^{l_n} = \left(\frac{f(n)}{p}\right) \quad \text{if} \quad f(n) \neq 0$$

and we have $f(n) = 0$ or $f(n+t) = 0$ for at most $2\deg(f)$ different n, with $0 \leq n < p$. Hence, for $1 \leq t < p$ and using the multiplicativity of the Legendre symbol, we have

$$p|\mathrm{AC}(\mathcal{L}, t)| \leq \left| \sum_{n=0}^{p-1} \left(\frac{f(n)f(n+t)}{p}\right) \right| + 2\deg(f)$$

and the result follows using the Weil bound.

The above lemma naturally holds for the classical case of Legendre sequences. This can be easily checked by instantiating the polynomial $f(X)$ with $f(X) = X$.

We state now the following existence result.

Corollary 1. *Let* $\mathcal{L} = (l_n)_{n\geq 0}$ *be a generalised Legendre sequence of period* p*, with the polynomial* $f(X) \in \mathbb{F}_p[X]$ *of degree at most*

$$\frac{p^{1/2}}{2}\left(1 - \frac{4}{(\log p)^c}\right)$$

for some $c > 0$*, such that, for any* $1 \leq t < p$, $f(X)(f(X+t))$ *is not a square for any* $1 \leq t < p$*. Assume that we are given a black-box that outputs* l_n *for every input integer* n*. Then there exists a quantum algorithm which computes* p *with an exponentially small probability in polynomial time.*

The result in the above corollary is an immediate consequence of Theorem 1.

In the currently available literature, some generalised Legendre sequences for particular polynomials f have been studied. For example, in the case $f(X) = X + s$, where s is a shift, quantum algorithms for finding the period p and the shift s are given in [2]. In the case p is known then $f(X)$ can be recovered in the general case using an algorithm of quantum query complexity $O(\deg(f))$; see [8].

For considerations on the autocorrelation for extensions of Legendre sequences of period q, with q an odd prime power, which are defined over the field $\mathbb{F}_q$ which a special, somewhat natural, ordering of the elements and the quadratic character of $\mathbb{F}_q$, see [7]. For sequences of period pq with two primes p and q see [1,3].

4.2 Generalised Sidelnikov Sequences

Classically, a Sidelnikov sequence $\mathcal{S} = (s_n)_{n\geq 0}$ is defined by

$$s_n = \begin{cases} 1 \text{ if } \eta(g^n + 1) = -1, \\ 0 \text{ otherwise,} \end{cases} \qquad n \geq 0,$$

where g is a *primitive element* and η denotes the *quadratic character* of the finite field $\mathbb{F}_q$ of odd order q.

Let q be an odd prime power, $f(X)$ a polynomial over the finite field $\mathbb{F}_q$ of q elements, and $g \in \mathbb{F}_q$ an element of order T. Then a *generalised Sidelnikov sequence* $\mathcal{S} = (s_n)_{n\geq 0}$ *of period* T*, with an element* g *of order* T *and a polynomial* f is defined by

$$s_n = \begin{cases} 1, \text{ if } \eta(f(g^n)) = -1, \\ 0, \text{ otherwise,} \end{cases} \qquad n \geq 0,$$

where η is, as before, the quadratic character of the field $\mathbb{F}_q$.

The following result is again based on the Weil bound.

Lemma 4. *Let* $\mathcal{S}$ *be a generalised Sidelnikov sequence of period* T*, with an element* $g \in \mathbb{F}_q$ *of order* T *and a polynomial* $f(X) \in \mathbb{F}_q[X]$ *such that, for any* $1 \leq t < T$*,* $f(X)f(g^tX)$ *is, up to a constant, not a square. Then we have*

$$\max_{1\leq t<T} |\mathrm{AC}(\mathcal{S}, t)| < 2\deg(f)(q^{1/2} + 1)T^{-1}.$$

Proof. The conclusion of the lemma follows immediately from the Weil's theorem. Namely, we have

$$\begin{aligned} &T|A(\mathcal{S}, t)| \\ &\leq \left| \sum_{n=0}^{T-1} \eta(f(g^n)f(g^tg^n)) \right| + 2\deg(f) \\ &\leq \frac{T}{q-1}\left(\left| \sum_{x\in\mathbb{F}_q} \eta(f(x^{(q-1)/T})f(g^tx^{(q-1)/T})) \right| + 1 \right) + 2\deg(f) \\ &\leq \frac{T}{q-1}(2\deg(f)(q-1)/T - 1)q^{1/2} + 2\deg(f) \\ &< 2\deg(f)(q^{1/2} + 1). \end{aligned}$$

As it was the case for Legendre sequences, Lemma 4 holds also for the classical case of Sidelnikov sequences. In order to check this we have to take $f(X) = X+1$.

Corollary 2. *Let $\mathcal{S} = (s_n)_{n\geq 0}$ be a generalised Sidelnikov sequence of period T, with $g \in \mathbb{F}_q$ of order T and a polynomial $f(X) \in \mathbb{F}_q[X]$ of degree at most*

$$\frac{T}{2(q^{1/2}+1)}\left(1 - \frac{4}{(\log T)^c}\right)$$

for some $c > 0$, such that, for any $1 \leq t < T$, $f(X)(f(g^tX))$ is, up to a constant, not a square. Assume that we are given a black-box which, for every integer n, outputs s_n. Then there exists a quantum algorithm which computes T in polynomial time with an exponentially small probability of failure.

4.3 Generalised Trace Sequences

Let us now look at generalisations of trace sequences. A *trace sequence* $\mathcal{T} = (t_n)_{n\geq 0}$ is defined by

$$t_n = \mathrm{Tr}\,(g^n), \quad n \geq 0,$$

where g is a primitive element of $\mathbb{F}_{2^r}$ and Tr denotes the *absolute trace* of $\mathbb{F}_{2^r}$, for some $r \geq 1$.

Let $f(X) \in \mathbb{F}_{2^r}[X]$, and $g \in \mathbb{F}_{2^r}$ an element of order T. We define the *generalised trace sequence $\mathcal{T} = (t_n)_{n\geq 0}$ of period T, with the polynomial f and element g* by

$$t_n = \mathrm{Tr}\,(f(g^n)), \quad n \geq 0.$$

The following result is based on Weil's bound for additive character sums; see, e.g., [6–Theorem 5.38].

Lemma 5. *For any generalised trace sequence $\mathcal{T} = (t_n)_{n\geq 0}$ of period T, with $g \in \mathbb{F}_{2^r}$ of order T and any polynomial $f(X) \in \mathbb{F}_{2^r}[X]$ such that $f(X)+f(g^tX)$ is not of the form $h(X)^2 + h(X) + c$ for any $1 \leq t < T$, we have*

$$\max_{1\leq t<T} |\mathrm{AC}(\mathcal{T}, t)| < \deg(f)2^{r/2}T^{-1}.$$

Corollary 3. *Let $\mathcal{T} = (t_n)_{n\geq 0}$ be a generalised trace sequence of period T, with $g \in \mathbb{F}_{2^r}$ of order T and any polynomial $f(X) \in \mathbb{F}_{2^r}[X]$ of degree at most*

$$\frac{T}{2^{r/2}}\left(1 - \frac{1}{(\log T)^c}\right),$$

for some $c > 0$ and such that $f(X)+f(g^tX)$ is not of the form $h(X)^2+h(X)+c$, for any $1 \leq t < T$. Assume that we are given a black-box which, for every integer n, gives t_n. Then there exists a quantum algorithm which computes T in polynomial time with an exponentially small probability of failure.

For some certain cases of trace sequences we can recover the period T also by combining the Berlekamp-Massey and the Shor algorithm. The Berlekamp-Massey algorithm delivers the coefficients $c_0, \ldots, c_L \in \mathbb{F}_2$ of the shortest linear recurrence relation

$$\sum_{l=0}^{L} c_l t_{n+l} = 0, \quad n \geq 0,$$

satisfied by $\mathcal{T}$. For example, if $f(X) = X$ this leads to

$$\operatorname{Tr}\left(g^n \sum_{l=0}^{L} c_l g^l\right) = 0, \quad n \geq 0.$$

We denote the sum above with b. If g is a defining element of $\mathbb{F}_{2^r}$, i.e., $\{1, \ldots, g^{r-1}\}$ is a basis of $\mathbb{F}_{2^r}$, then by the linearity of the trace $\operatorname{Tr}(bg^n) = 0$, $0 \leq n < r$, we know that $\operatorname{Tr}(bx) = 0$, $x \in \mathbb{F}_{2^r}$, and thus $b = 0$. A root finding algorithm can be used to determine g and, finally, Shor's algorithm can be applied to calculate T.

4.4 Elliptic Curve Trace Sequences

Let E be an elliptic curve over $\mathbb{F}_{2^r}$ and P a rational point on E of order T. For a function f in the function field $\mathbb{F}_{2^r}(E)$ the sequence $\mathcal{E} = (e_n)_{n\geq 0}$ defined by $e_n = \operatorname{Tr}(f(nP))$, $n \geq 0$, has the period T.

The following result follows from [5–Corollary 1].

Lemma 6. *For any function f in the function field $\mathbb{F}_{2^r}(E)$ such that $f(nP) - f((n+t)P)$ is not constant for $1 \leq t < T$ and $n \geq 0$, the sequence $\mathcal{E} = (e_n)_{n\geq 0}$ satisfies*

$$\max_{1\leq t<T} |\mathrm{AC}(\mathcal{E}, t)| \leq 4 \deg(f) 2^{r/2} T^{-1}.$$

For example, the function $f(Q) = x(Q)$, where $x(Q)$ is the first coordinate of $Q = (x(Q), y(Q)) \in E$, satisfies the condition that $s_n - s_{n+t} = f(nP) - f((n+t)P)$ is not constant, for $1 \leq t < T$.

Corollary 4. *Let $\mathcal{E} = (e_n)_{n\geq 0}$ be a sequence of period T defined as in Lemma 6 with* $\deg(f)$ *at most*

$$\frac{T}{4 \cdot 2^{r/2}} \left(1 - \frac{4}{(\log 2^r)^c}\right)$$

for some $c > 0$. Assume that we are given a black-box which for every integer n outputs e_n. Then there exists a quantum algorithm which computes T in polynomial time with an exponentially small probability of failure.

Acknowledgements. A. W. was supported in part by the Austrian Academy of Sciences and by FWF grant S8313. The authors wish to thank Igor Shparlinski for helpful comments.

References

1. N. Brandstätter and A. Winterhof. Some notes on the two-prime generator of order 2. *IEEE Trans. Inform. Theory*, **51**, 3654–3657, 2005.
2. W. van Dam, S. Hallgren and L. Ip. Quantum algorithms for some hidden shift problems. *Proc. of the 14th Annual ACM-SIAM Symposium on Discrete Algorithms, Baltimore, 2003*, 489–498, ACM, New York, 2003.
3. C. Ding. Autocorrelation values of generalized cyclotomic sequences of order two. *IEEE Trans. Inform. Theory*, **44**, 1699–1702, 1998.
4. L. Hales and S. Hallgren. An improved quantum Fourier transform algorithm and applications. *Proc. 41st IEEE Symp. on Found. of Comp. Sci.*, 515–525, 2000.
5. D. R. Kohel and I. E. Shparlinski. Exponential sums and group generators for elliptic curves over finite fields. *Proc. of the 4th International Symposium on Algorithmic Number Theory*, Lecture Notes in Computer Science, **1838**, 395–404, Springer-Verlag, London, UK, 2000.
6. R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.
7. W. Meidl and A. Winterhof. On the autocorrelation of cyclotomic generators. *Finite Fields and Applications: 7th International Conference, Fq7, Toulouse, France, May 5-9, 2003*, Lecture Notes in Computer Science, **2948**, 1–11, Springer, Berlin, 2004.
8. A. Russell and I. E. Shparlinski. Classical and quantum function reconstruction via character evaluation. *J. Complexity* **20**, 404–422, 2004.
9. P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comp.*, **26**, 1484–1509, 1997.
10. I. Shparlinski and A. Winterhof. Quantum period reconstruction of noisy sequences. *Proc. ERATO Conf. on Quantum Inform. Sci.*, Tokyo, 2005, 7–8.