On a family of linear recurrences

2013 J. Phys.: Conf. Ser. 410 012057

(http://iopscience.iop.org/1742-6596/410/1/012057)

IC-MSQUARE 2012: International Conference on Mathematical Modelling in Physical Sciences IOP Publishing
Journal of Physics: Conference Series **410** (2013) 012057 doi:10.1088/1742-6596/410/1/012057

On a family of linear recurrences

C M Wilmott

Faculty of Informatics, Masaryk University, Šumavská 416/15, 602 00 Brno, Czech Republic

E-mail: wilmott@fi.muni.cz

Abstract. We concern ourselves with the family of linear recurrence relations $a_j = a_{j-1} + a_{j-d}$ with the initial conditions $a_0 = \ldots = a_{d-1} = 1$. We discuss the periodicity evaluation of such recurrences for prime powers d, and demonstrate that a key feature of our evaluation method relates to an instance of Shor's algorithm for factoring. As an application, we discuss how efficient quantum circuit designs may be completely recast as a problem relating to linear recurrence relations.

1. Introduction

Recurrence relations possess a rich history with applications extending from biology to economics. Indeed, many algorithms have time complexities that can be modelled by recurrence relations. In this paper, we will discuss a family of d^{th}-order linear recurrence relations before revealing a novel application to quantum circuit designs. Our main result focuses on the task of evaluating the periodicity of a family of recurrence relations.

Let d be a positive integer and consider the recurrence relation

$$a_j = a_{j-1} + a_{j-d} + [j = 0] \pmod{d} \tag{1}$$

where $[j = 0]$ adds 1 when $j = 0$. The solution to this recurrence relation is given by the binomial summation

$$a_j = \sum_{i=0}^{j/d} \binom{j-(d-1)i}{i}, \tag{2}$$

and, furthermore, its closed-form is given by

$$a_j = \sum_{l=1}^{d} \beta_l \alpha_l^j, \tag{3}$$

where α_l denote the reciprocals of the roots of $B(z) = 1 - z - z^d$ and $\beta_l = -\alpha_l / B'(1/\alpha_l)$ [1]. For d prime, the periodicity of the recurrence relation is $d^2 - 1$. For the prime power case $d = p^m$ with p prime, the periodicity of this recurrence relation remains an open problem, however, it is conjectured to be $p^{m-1}(p^{2m} - 1)$ [1].

Interestingly, Wilmott [1] established that the periodic property of recurrence relations can be used to study the computational problem associated with the construction of certain quantum

circuits possessing an exact number of constituent gates; in particular, quantum SWAP gates with a minimal number of CNOT gates. Crucially, however, the answer to this question directly depends on knowing the periodicity for the family of recurrence relations presented in Eq. (1). We now present some preliminary material before progressing to our main result.

2. Recurrence relations and Shor's Algorithm

Consider a d-dimensional complex Hilbert space $\mathbb{C}^d$ and fix each orthonormal basis state of the d-dimensional space to correspond to an element of ring $\mathbb{Z}_d$ of integers modulo d. The basis elements $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\} \subset \mathbb{C}^d$ correspond to the column vectors of the identity matrix $\mathbb{I}_d$ and is called the computational basis. A qudit is then a d-dimensional quantum state $|\psi\rangle \in \mathbb{C}^d$ written $|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle$ where $\alpha_i \in \mathbb{C}$ and $\sum_{i=0}^{d-1} |\alpha_i|^2 = 1$. An n-qudit state is the tensor product of the basis states of the single system $\mathbb{C}^d$; $(\mathbb{C}^d)^{\otimes n}$, and its basis states are $|i_1\rangle \otimes |i_2\rangle \otimes \ldots \otimes |i_n\rangle = |i_1 i_2 \ldots i_n\rangle$ where $i_j \in \mathbb{Z}_d$. Further, the CNOT gate is a two-qudit quantum gate whose action on the basis states $|i\rangle \otimes |j\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ is given by

$$\text{CNOT} |i\rangle \otimes |j\rangle = |i\rangle \otimes |j \oplus i\rangle, \qquad i, j \in \mathbb{Z}_d, \tag{4}$$

with $\oplus$ denoting addition modulo d. We will now outline how Shor's algorithm [2] can be used to confirm the conjecture relating the period of the recurrence relation presented in Eq. (1).

Consider an initial state written as a composition of two registers;

$$|\Psi_0\rangle = |0\rangle |1, 1, \ldots, 1\rangle. \tag{5}$$

The first register is prepared in the zero state while the second register is prepared as a collection of d one states. For $d = p^m$, let $r = p^{m-1}(p^{2m} - 1)$ be the period of the recurrence relation in Eq. (1), and choose an $n \in \mathbb{N}$ such that r divides d^n. Placing the first register in a uniform superposition of states representing integers a mod d^n, we have

$$|\Psi_1\rangle = \frac{1}{\sqrt{d^n}} \sum_{a=0}^{d^n-1} |a\rangle |1, 1, \ldots, 1\rangle. \tag{6}$$

Focusing on the second register of Eq. (6), let us define a set of states $|\mathrm{u}_s\rangle$ by

$$|\mathrm{u}_s\rangle := \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi\iota ks/r} \left| \sum_{l=1}^{d} \beta_l \alpha_l^k, \sum_{l=1}^{d} \beta_l \alpha_l^{k+1}, \ldots, \sum_{l=1}^{d} \beta_l \alpha_l^{k+d-1} \pmod d \right\rangle \tag{7}$$

with $0 \leq s < r$. Following the style style presented in Nielsen & Chuang [3], we exploit the fact that a suitable combination of such states $|\mathrm{u}_s\rangle$ yields the state of the second register. In particular,

$$\begin{aligned} \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\mathrm{u}_s\rangle &= \frac{1}{r} \sum_{s=0}^{r-1} \sum_{k=0}^{r-1} e^{-2\pi\iota ks/r} \left| \sum_{l=1}^{d} \beta_l \alpha_l^k, \sum_{l=1}^{d} \beta_l \alpha_l^{k+1}, \ldots, \sum_{l=1}^{d} \beta_l \alpha_l^{k+d-1} \pmod d \right\rangle \\ &= \sum_{k=0}^{r-1} \delta_{k,0} \left| \sum_{l=1}^{d} \beta_l \alpha_l^k, \sum_{l=1}^{d} \beta_l \alpha_l^{k+1}, \ldots, \sum_{l=1}^{d} \beta_l \alpha_l^{k+d-1} \pmod d \right\rangle \\ &= |1, 1, \ldots, 1\rangle. \end{aligned} \tag{8}$$

Next, we define a unitary transformation $\Lambda(U) := I \otimes U^a$ which acts according to the circuit of Fig. 1. The unitary transformation $\Lambda(U)$ is a controlled-U^a operation and acts on the state of

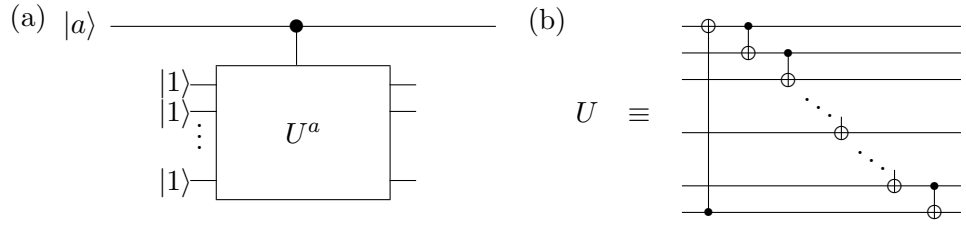

Figure 1. (a) The unitary transformation $\Lambda(U)$ is represented as a controlled-U^a operation. When the state of the first register is $|a\rangle$, an a-fold product of U is applied to the second register. (b) The transformation U consist of d CNOT gates which produce clock cycles of length d of the recurrence relation given in Eq. (1).

the second register. The effect of $\Lambda(U)$ is to produce a set of disjoint cycles of coefficients of length d related to the recurrence relation of Eq. (1). For example, when the state of the first register is one, $\Lambda(U)$ will act on the state $|1\rangle|\mathrm{u}_s\rangle$ by applying a set of d CNOT gates conditioned on successive states of the target register. The effect of these gates mimics the action of the recurrence relation transforming the second register from $|a_0, a_1 \ldots, a_{d-1}\rangle$ to $|a_d, a_{d+1}, \ldots, a_{2d-1}\rangle$;

$$\begin{aligned}
&\Lambda(U)|1\rangle|\mathrm{u}_s\rangle = |1\rangle U^1|\mathrm{u}_s\rangle \\
&= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi\iota ks/r}|1\rangle U\left|\sum_{l=1}^{d}\beta_l\alpha_l^k, \sum_{l=1}^{d}\beta_l\alpha_l^{k+1}, \ldots, \sum_{l=1}^{d}\beta_l\alpha_l^{k+d-1} \pmod d\right\rangle \\
&= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi\iota ks/r}|1\rangle\left|\sum_{l=1}^{d}\beta_l\alpha_l^{k+d}, \sum_{l=1}^{d}\beta_l\alpha_l^{k+d+1}, \ldots, \sum_{l=1}^{d}\beta_l\alpha_l^{k+2d-1} \pmod d\right\rangle. \qquad (9)
\end{aligned}$$

When the shift invariance property of the Fourier transform is applied to Eq. (9), it is readily established that input state $|1\rangle|\mathrm{u}_s\rangle$ is an eigenstate of $\Lambda(U)$;

$$\begin{aligned}
&\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi\iota(k-d)s/r}|1\rangle\left|\sum_{l=1}^{d}\beta_l\alpha_l^k, \sum_{l=1}^{d}\beta_l\alpha_l^{k+1}, \ldots, \sum_{l=1}^{d}\beta_l\alpha_l^{k+d-1} \pmod d\right\rangle \\
&= e^{2\pi\iota ds/r}|1\rangle|\mathrm{u}_s\rangle. \qquad (10)
\end{aligned}$$

More generally, it can be shown that $|a\rangle|\mathrm{u}_s\rangle$ is also an eigenstate of $\Lambda(U)$ and, as such, we have it that $\Lambda(U)|a\rangle|\mathrm{u}_s\rangle = |a\rangle U^a|\mathrm{u}_s\rangle = e^{2\pi\iota ads/r}|a\rangle|\mathrm{u}_s\rangle$. Noting this, we apply $\Lambda(U)$ to state $|\Psi_1\rangle$;

$$\begin{aligned}
&\Lambda(U)|\Psi_1\rangle = \Lambda(U)\left(\frac{1}{\sqrt{d^n}}\sum_{a=0}^{d^n-1}|a\rangle|11\ldots1\rangle\right) \\
&= \Lambda(U)\left(\frac{1}{\sqrt{d^n}r}\sum_{a=0}^{d^n-1}\sum_{s=0}^{r-1}\sum_{k=0}^{r-1} e^{-2\pi\iota ks/r}|a\rangle\left|\sum_{l=1}^{d}\beta_l\alpha_l^k, \sum_{l=1}^{d}\beta_l\alpha_l^{k+1}, \ldots, \sum_{l=1}^{d}\beta_l\alpha_l^{k+d-1} \pmod d\right\rangle\right) \\
&= \frac{1}{\sqrt{d^n}r}\sum_{a=0}^{d^n-1}\sum_{s=0}^{r-1}\sum_{k=0}^{r-1} e^{-2\pi\iota ks/r}|a\rangle U^a\left|\sum_{l=1}^{d}\beta_l\alpha_l^k, \sum_{l=1}^{d}\beta_l\alpha_l^{k+1}, \ldots, \sum_{l=1}^{d}\beta_l\alpha_l^{k+d-1} \pmod d\right\rangle \\
&= \frac{1}{\sqrt{d^n}r}\sum_{a=0}^{d^n-1}\sum_{s=0}^{r-1}\sum_{k=0}^{r-1} e^{-2\pi\iota ks/r}|a\rangle\left|\sum_{l=1}^{d}\beta_l\alpha_l^{k+ad}, \sum_{l=1}^{d}\beta_l\alpha_l^{k+ad+1}, \ldots, \sum_{l=1}^{d}\beta_l\alpha_l^{k+(a+1)d-1} \pmod d\right\rangle. \qquad (11)
\end{aligned}$$

The sequence values recorded in the second register is periodic as the recurrence relation is reversible and must repeat as soon as d consecutive terms, of which there are only finitely

many possibilities, are repeated. Therefore, there exists an $a = jr + l$ for some $1 \leq l < r$ and $0 \leq j < d^n/r$ such that Eq. (11) can be written as

$$\frac{1}{\sqrt{d^n r}} \sum_{j=0}^{d^n/r-1} \sum_{l=0}^{r-1} \sum_{s=0}^{r-1} \sum_{k=0}^{r-1} e^{-2\pi\iota ks/r} \left|jr+l\right\rangle \left| \sum_{l=1}^{d} \beta_l \alpha_l^{k+(jr+l)d}, \ldots, \sum_{l=1}^{d} \beta_l \alpha_l^{k+(jr+l+1)d-1} \pmod d \right\rangle. \quad (12)$$

Applying the shift invariance property of the Fourier transform yields

$$\frac{1}{\sqrt{d^n r}} \sum_{j=0}^{d^n/r-1} \sum_{l=0}^{r-1} \sum_{s=0}^{r-1} \sum_{k=0}^{r-1} e^{-2\pi\iota (k-(jr+l)d)s/r} \left|jr+l\right\rangle \left| \sum_{l=1}^{d} \beta_l \alpha_l^{k}, \ldots, \sum_{l=1}^{d} \beta_l \alpha_l^{k+d-1} \pmod d \right\rangle \quad (13)$$

and, by definition of $|\mathrm{u}_s\rangle$, we can simplify Eq. (13) to

$$\frac{1}{\sqrt{d^n r}} \sum_{j=0}^{d^n/r-1} \sum_{l=0}^{r-1} \sum_{s=0}^{r-1} e^{2\pi\iota (jr+l)ds/r} \left|jr+l\right\rangle \left|\mathrm{u}_s\right\rangle. \quad (14)$$

Implementing the inverse Fourier transform on the first register transforms Eq. (14) to

$$\frac{1}{d^n \sqrt{r}} \sum_{m=0}^{d^n-1} \sum_{j=0}^{d^n/r-1} \sum_{l=0}^{r-1} \sum_{s=0}^{r-1} e^{2\pi\iota j(ds-mr/d^n)} e^{2\pi\iota l(ds/r-m/d^n)} \left|m\right\rangle \left|\mathrm{u}_s\right\rangle. \quad (15)$$

Now, noting that

$$\sum_{j=0}^{d^n/r-1} \left(e^{2\pi\iota(ds-mr/d^n)}\right)^j = \begin{cases} d^n/r & \text{if } e^{2\pi\iota(ds-mr/d^n)} = 1 \\ 0 & \text{otherwise} \end{cases}. \quad (16)$$

However, $e^{2\pi\iota(ds-mr/d^n)} = 1$ if and only if $ds - mr/d^n$ is an integer. Therefore, m must be a multiple of d^n/r. Thus, the state of the system can be given as

$$\frac{1}{r\sqrt{r}} \sum_{c=0}^{r-1} \sum_{l=0}^{r-1} \sum_{s=0}^{r-1} e^{2\pi\iota l(ds-c)/r} \left|cd^n/r\right\rangle \left|\mathrm{u}_s\right\rangle. \quad (17)$$

Again, since $\sum_{l=0}^{r-1} e^{2\pi\iota l(ds-c)/r} = r\delta_{ds-c,0}$, it follows that Eq. (17) can be written as

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left|sd^{n+1}/r\right\rangle \left|\mathrm{u}_s\right\rangle. \quad (18)$$

Finally measuring the first register, we find an m equal to sd^{n+1}/r for some integer s with $0 \leq s < r$. Since both m and d^{n+1} are known, the value r can be confirmed by writing m/d^{n+1} in its lowest form.

3. Conclusion

We discussed the problem of determining the period of a family of linear recurrences and related this problem to a particular instance of Shor's algorithm for factoring.

References

[1] Wilmott C M 2008 *On quantum codes and networks* Ph.D. Thesis Royal Holloway University of London
[2] Shor P W 1997 *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer* SIAM Journal on Computing **26** 5 1484-1509
[3] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* Cambridge University Press