LIÈGE université Mathematics

fnrs FREEDOM TO RESEARCH

Magic Numbers in Periodic Sequences

Manon Stipulanti

Joint work with Savinien Kreczman (ULiège, Belgium)
Luca Prigioniero (Unimi, Italy)
Eric Rowland (Hofstra University, USA)

14th International Conference on WORDS
Umeå, Sweden
June 12th, 2023

Notation and Vocabulary

- period length of s smallest $\ell \geq 1$ s.t. $s(n+\ell) = s(n) \quad \forall n \geq 0$
- $\mathsf{Per}(\ell) = \{\text{periodic sequences with period length } \ell\}$
- $(s(0), s(1), \ldots, s(\ell-1))$ period of $s \in \mathsf{Per}(\ell)$

Example: $s \in \mathsf{Per}(12)$ period $(0, 4, 5, 1, 4, 6, 2, 4, 5, 3, 4, 6)$

	period	period length
$s(n)$	$(0, 4, 5, 1, 4, 6, 2, 4, 5, 3, 4, 6)$	12
$s(3n)$	$(0, 1, 2, 3)$	4
$s(3n+1)$	(4)	1 (constant)
$s(3n+2)$	$(5, 6)$	2
$s(9n)$	$(0, 3, 2, 1)$	4

Lemma

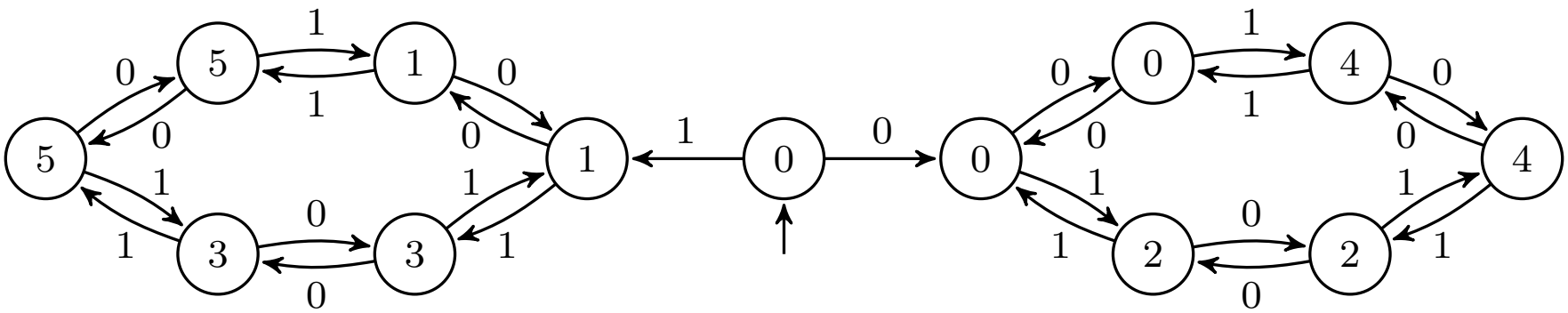
If the period length of s divides ℓ, that of $s(cn+r)_{n\geq 0}$ divides $\frac{\ell}{\gcd(c,\ell)}$

Theorem (Büchi, 1960)

Every periodic sequence is k-automatic

- s is k-automatic if there exists a DFAO producing s in base k

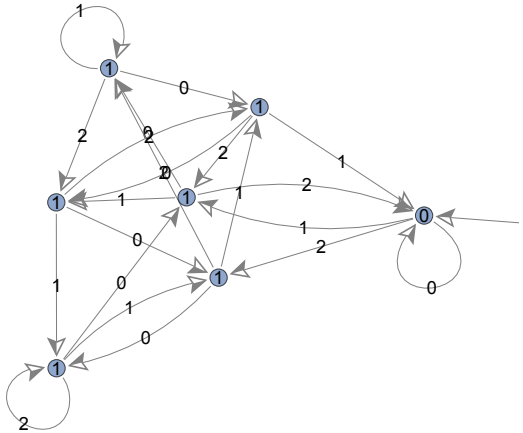
Example: $s \in \mathsf{Per}(6)$ period $(0, 1, 2, 3, 4, 5)$ 2-automatic



n	base-2 digits	output
0	ε	0
1	1	1
2	10	2
3	11	3
42	101010	0

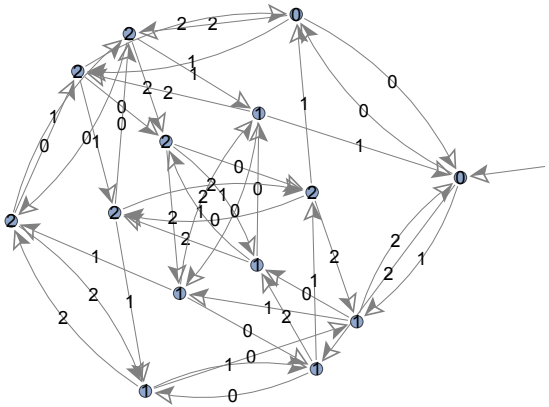
Per(7) versus 3-Automatic

$(0, 1, 1, 1, 1, 1, 1)$



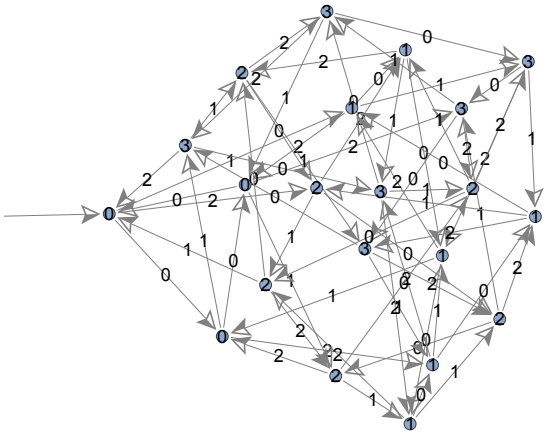
size 7

$(0, 1, 1, 2, 1, 2, 2)$



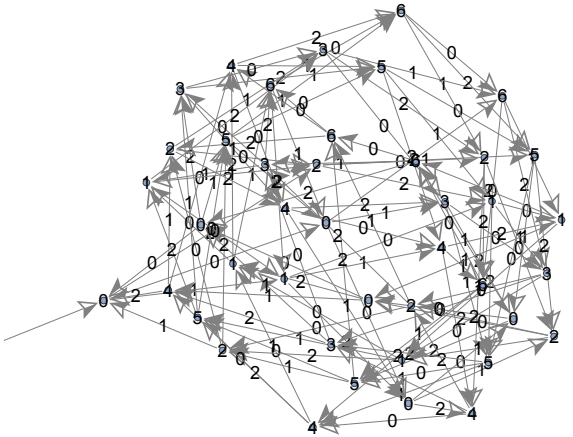
size 14

$(0, 1, 2, 3, 3, 2, 1)$



size 21

$(0, 1, 2, 3, 4, 5, 6)$



size 42

Question: Can we characterize these sizes?

Wizardry: Magic Number Problem

- integers $k, \ell \geq 2$
- family $\mathsf{Per}(\ell)$
- n satisfies property $\mathrm{P_a}(k, \ell)$ if $\exists s \in \mathsf{Per}(\ell)$ s.t. $n =$ size DFAO for s

Muggle number

$\mathrm{P_a}(k, \ell)$ ✓

Magic number

$\mathrm{P_a}(k, \ell)$ ✗

- range smallest interval $\supseteq$ all muggle numbers

Goal: for $\mathrm{P_a}(k, \ell)$, determine

- the range
- the muggle and magic numbers

Kernel

set of states in the minimal DFAO for $s \leftrightharpoons \text{kernel}_k(s)$

- $\text{kernel}_k(s) = \{s(k^e n + j)_{n \geq 0} : e \geq 0 \text{ and } 0 \leq j \leq k^e - 1\}$
- $\text{rank}_k(s) = |\text{kernel}_k(s)|$

Example: $s \in \mathsf{Per}(6)$ period $(0, 1, 2, 3, 4, 5)$

$\text{kernel}_2(s)$

(e, j)	period of $s(2^e n + j)_{n \geq 0}$
$(0, 0)$	$(0, 1, 2, 3, 4, 5)$
$(1, 0), (3, 0), (3, 6)$	$(0, 2, 4)$
$(1, 1), (3, 1), (3, 7)$	$(1, 3, 5)$
$(2, 0), (4, 0), (4, 6), (4, 12)$	$(0, 4, 2)$
$(2, 1), (4, 1), (4, 7), (4, 13)$	$(1, 5, 3)$
$(2, 2), (4, 2), (4, 8), (4, 14)$	$(2, 0, 4)$
$(2, 3), (4, 3), (4, 9), (4, 15)$	$(3, 1, 5)$
$(3, 2)$	$(2, 4, 0)$
$(3, 3)$	$(3, 5, 1)$
$(3, 4)$	$(4, 0, 2)$
$(3, 5)$	$(5, 1, 3)$
$(4, 4), (4, 10)$	$(4, 2, 0)$
$(4, 5), (4, 11)$	$(5, 3, 1)$

$\text{rank}_2(s) = 13$

Range for $\mathrm{P_a}(k, \ell)$

$(k^e \bmod \ell)_{e \geq 0}$ preperiod length $\mathrm{pre}_\ell(k)$ period length $\mathrm{ord}_\ell(k)$

Example: $\ell = 7$ $k = 3$ $(3^e \bmod 7)_{e \geq 0} = 1, 3, 2, 6, 4, 5, 1, 3, 2, 6, 4, 5, \ldots$

case	bound
general	upper $B_\ell(k) = \ell \cdot \mathrm{ord}_\ell(k) + \sum_{e=0}^{\mathrm{pre}_\ell(k)-1} \min(k^e, \ell)$ Ex: $(0, 1, \ldots, \ell - 1)$
coprime	lower ℓ Ex: $(0, 0, \ldots, 0, 1)$

Proposition

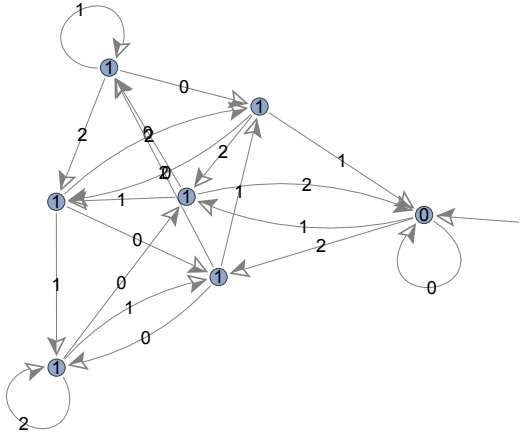
All muggle numbers belong to $[\ell, B_\ell(k)]$ if k and ℓ are coprime

Example:

		k					
		2	3	4	5	6	7
	2		$[2, 2]$		$[2, 2]$		$[2, 2]$
	3	$[3, 6]$		$[3, 3]$	$[3, 6]$		$[3, 3]$
ℓ	4		$[4, 8]$	$[4, 4]$			$[4, 8]$
	5	$[5, 20]$	$[5, 20]$	$[5, 10]$		$[5, 5]$	$[5, 20]$
	6				$[6, 12]$		$[6, 6]$
	7	$[7, 21]$	$[7, 42]$	$[7, 21]$	$[7, 42]$	$[7, 14]$	

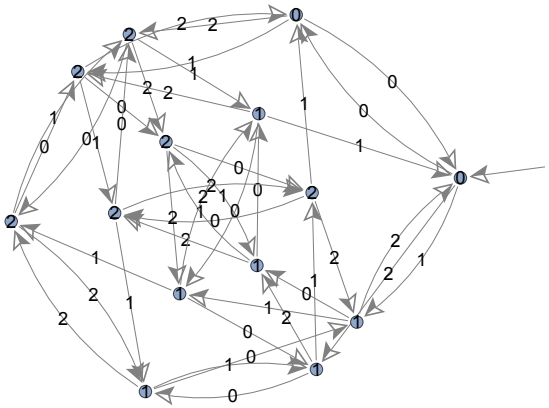
3-Automatic versus Per(7)

$(0, 1, 1, 1, 1, 1, 1)$



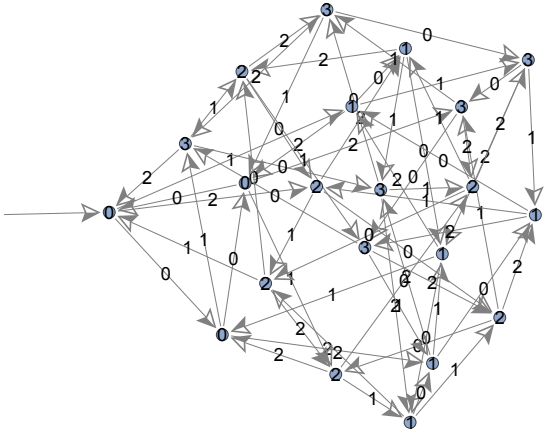
size 7

$(0, 1, 1, 2, 1, 2, 2)$



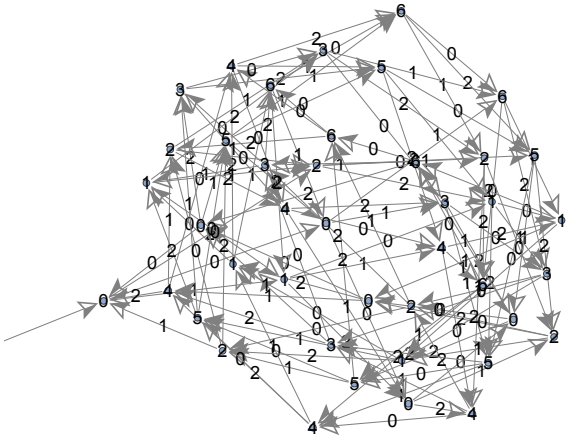
size 14

$(0, 1, 2, 3, 3, 2, 1)$



size 21

$(0, 1, 2, 3, 4, 5, 6)$



size 42

Muggle and Magic Numbers for $\mathrm{P_a}(k, \ell)$

Theorem

Let k and ℓ be coprime. For $\mathrm{P_a}(k, \ell)$

$$A = \{d\ell : d \in \mathsf{Div}(\mathrm{ord}_\ell(k))\}$$

$$\mathbb{N} \setminus A$$

constructive proof

Example: $\ell = 7 \;\; k = 3 \;\; (3^e \bmod 7)_{e \geq 0} = 1, 3, 2, 6, 4, 5, 1, 3, 2, 6, 4, 5, \ldots$

$$\mathrm{pre}_3(7) = 0 \quad \mathrm{ord}_3(7) = 6$$
$$A = \{7d : d \in \mathsf{Div}(6)\}$$

d	$\mathrm{rank}_3(s)$	period of s
6	42	$(0, 1, 2, 3, 4, 5, 6)$
3	21	$(0, 1, 2, 3, 3, 2, 1)$
2	14	$(0, 1, 1, 2, 1, 2, 2)$
1	7	$(0, 1, 1, 1, 1, 1, 1)$

Constant-Recursive Sequences

Remark

Every periodic sequence is constant-recursive

- s is constant recursive if $\exists\, c_0, c_1, \ldots, c_{d-1} \in \mathbb{Z}$ with $c_0 \neq 0$ s.t.

$$s(n+d) = c_{d-1}s(n+d-1) + \cdots + c_1 s(n+1) + c_0 s(n) \quad \forall n \geq 0$$

Example:

$s \in \mathsf{Per}(6)$ period $(0,1,2,3,4,5)$	$s \in \mathsf{Per}(3)$ period $(-1,0,1)$
$s(n+6) = s(n)$	$s(n+3) = s(n)$ $s(n+2) = -s(n+1) - s(n)$

- $\mathrm{rank}(s) =$ smallest d

$\mathrm{rank}(s) = |\ker_1(s)| \quad \ker_1(s) = \{s(n+j)_{n\geq 0} : j \geq 0\}$

Example:

$\mathrm{rank}(s) = 6$	$\mathrm{rank}(s) = 2$

- integer $\ell \geq 2$
- family $\mathsf{Per}(\ell)$
- n satisfies property $\mathrm{P_{cr}}(\ell)$ if $\exists s \in \mathsf{Per}(\ell)$ s.t. $n = \mathrm{rank}(s)$

Muggle number

$\mathrm{P_{cr}}(\ell)$ ✓

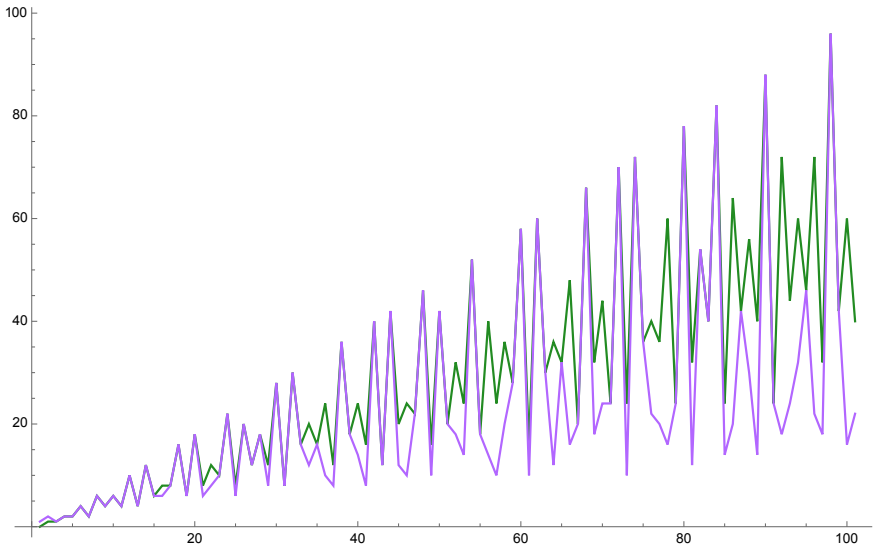
Magic number

$\mathrm{P_{cr}}(\ell)$ ✗

Goal: for $\mathrm{P_{cr}}(\ell)$, determine

- the range
- the muggle and magic numbers

Range for $P_{cr}(\ell)$



Euler totient function ϕ

additive version ψ

- p prime, $k \geq 1$: $\psi(p^k) = \phi(p^k)$
- n odd: $\psi(2n) = \phi(n)$
- m, n relatively prime, $\neq 2$: $\psi(mn) = \phi(m)+\phi(n)$

Proposition

All muggle numbers belong to $[\psi(\ell), \ell]$

Example:

ℓ	2	3	4	5	6	7	8
$[\psi(\ell), \ell]$	$[1, 2]$	$[2, 3]$	$[2, 4]$	$[4, 5]$	$[2, 6]$	$[6, 7]$	$[4, 8]$
ℓ	9	10	11	12	13	14	15
$[\psi(\ell), \ell]$	$[6, 9]$	$[4, 10]$	$[10, 11]$	$[4, 12]$	$[12, 13]$	$[6, 14]$	$[6, 15]$

Muggle and Magic Numbers for $\mathrm{P}_{\mathrm{cr}}(\ell)$

Theorem

S: $\emptyset \neq \{d_1, \ldots, d_j\} \subset \mathbb{N}$ pairwise distinct s.t. $\mathrm{lcm}(d_1, \ldots, d_j) = \ell$
For $\mathrm{P}_{\mathrm{cr}}(\ell)$

$R = \{\sum_{i=1}^{j} \phi(d_i) : \{d_1, \ldots, d_j\} \in S\}$

$\mathbb{N} \setminus R$

constructive proof

Example: $\ell = 6$

$\{d_1, \ldots, d_j\}$	rank(s)	char. poly	period of s
$\{6\}$	2	$x^2 - x + 1$	$(0, 1, 1, 0, -1, -1)$
$\{2, 3\}$	3	$x^3 + 2x^2 + 2x + 1$	$(0, 0, 1, -2, 2, -1)$
$\{3, 6\}$	4	$x^4 + x^2 + 1$	$(0, 0, 0, 1, 0, -1)$
$\{2, 3, 6\}$	5	$x^5 + x^4 + x^3 + x^2 + x + 1$	$(0, 0, 0, 0, 1, -1)$
$\{1, 2, 3, 6\}$	6	$x^6 - 1$	$(0, 0, 0, 0, 0, 1)$

Remark

Automatic sequences are regular $\rightsquigarrow$ Periodic sequences are regular

- s is k-regular if the $\mathbb{Q}$-vector space generated by $\text{kernel}_k(s)$ is finitely generated
- $\text{rank}_k(s)$ = dimension of the vector space

Example: $s \in \mathsf{Per}(4)$ period $(0,1,1,1)$

$$\underbrace{(0,1,1,1),(0,1),(1)}_{\text{lin. indep.}},\ (0) \qquad \text{kernel}_2(s)$$

	2-regular	2-automatic
$\text{rank}_2(s)$	3	4

Range, Muggle and Magic Numbers for $\mathrm{P_r}(k, \ell)$

- integers $k, \ell \geq 2$
- family $\mathsf{Per}(\ell)$
- n satisfies property $\mathrm{P_r}(k, \ell)$ if $\exists s \in \mathsf{Per}(\ell)$ s.t. $n = \mathrm{rank}_k(s)$

Theorem

All muggle numbers belong to $[\psi(\ell), \ell]$ if k and ℓ are coprime

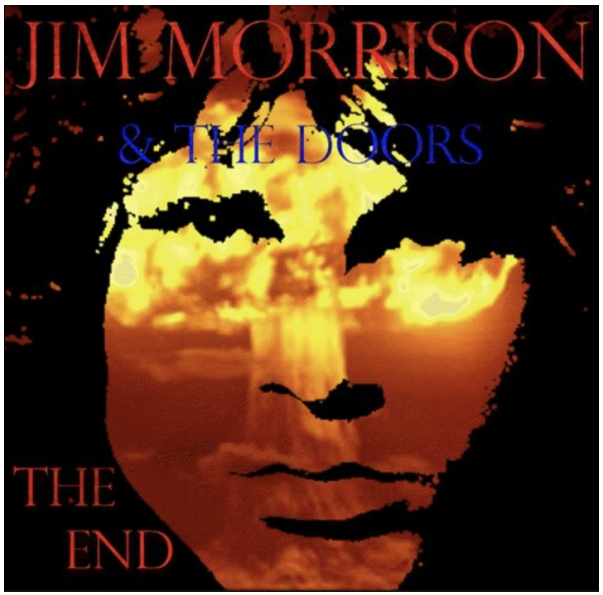
S: $\emptyset \neq \{d_1, \ldots, d_j\} \subset \mathbb{N}$ pairwise distinct s.t. $\mathrm{lcm}(d_1, \ldots, d_j) = \ell$
For $\mathrm{P_r}(k, \ell)$

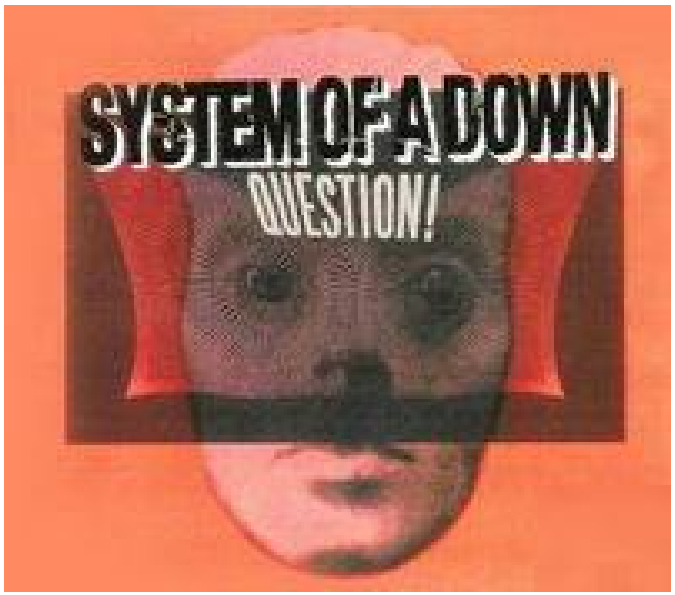
$R = \{\sum_{i=1}^{j} \phi(d_i) : \{d_1, \ldots, d_j\} \in S\}$

$\mathbb{N} \setminus R$

Conclusion

		automatic	constant-recursive	regular
range	general	?	✓	?
	coprime	✓	✓	✓
charact.	general	?	✓	?
	coprime	✓	✓	✓





References I

B. Alexeev.

Minimal DFA for testing divisibility.
J. Comput. Syst. Sci., 69(2):235–243, 2004.

J.-P. Allouche and J. O. Shallit.

The ring of k-regular sequences.
Theor. Comput. Sci., 98(2):163–197, 1992.

J.-P. Allouche and J. O. Shallit.

Automatic Sequences: Theory, Applications, Generalizations.
Cambridge University Press, 2003.

J. Bamberg, G. Cairns, and D. Kilminster.

The crystallographic restriction, permutations, and Goldbach's conjecture.
Am. Math. Mon., 110(3):202–209, 2003.

J. Berstel and C. Reutenauer.

Noncommutative rational series with applications, volume 137 of Encyclopedia of Mathematics and its Applications.
Cambridge University Press, Cambridge, 2011.

B. Boigelot, I. Mainz, V. Marsault, and M. Rigo.

An efficient algorithm to decide periodicity of b-recognisable sets using MSDF convention.
In ICALP 2017, volume 80 of LIPIcs, pages 118:1–118:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017.

W. Bosma.

Complexity of periodic sequences.
Preprint available at https://www.math.ru.nl/ bosma/pubs/periodic.pdf, 2019.

References II

R. J. Büchi.
Weak second-order arithmetic and finite automata.
Mathematical Logic Quarterly, 6(1-6):66–92, 1960.

A. Cobham.
Uniform tag sequences.
Math. Systems Theory, 6:164–192, 1972.

G. Everest, A. J. van der Poorten, I. E. Shparlinski, and T. Ward.
Recurrence sequences, volume 104 of Mathematical surveys and monographs.
American Mathematical Society, 2003.

P. B. Garrett.
Abstract algebra.
Chapman & Hall/CRC, Boca Raton, FL, 2008.

V. Geffert.
(Non)determinism and the size of one-way finite automata.
In 7th International Workshop on Descriptional Complexity of Formal Systems - DCFS 2005, Como, Italy, June 30 - July 2, 2005. Proceedings, pages 23–37. Università degli Studi di Milano, Milan, Italy, 2005.

V. Geffert.
Magic numbers in the state hierarchy of finite automata.
Inform. and Comput., 205(11):1652–1670, 2007.

References III

H. Hiller.
The crystallographic restriction in higher dimensions.
Acta Crystallographica Section A, 41(6):541–544, 1985.

M. Holzer, S. Jakobi, and M. Kutrib.
The magic number problem for subregular language families.
Int. J. Found. Comput. Sci., 23(1):115–131, 2012.

J. Honkala.
A decision method for the recognizability of sets defined by number systems.
RAIRO Theor. Informatics Appl., 20(4):395–403, 1986.

A. W. Ingleton.
The rank of circulant matrices.
J. London Math. Soc., 31:632–635, 1956.

K. Iwama, Y. Kambayashi, and K. Takaki.
Tight bounds on the number of states of DFAs that are equivalent to n-state NFAs.
Theoret. Comput. Sci., 237(1-2):485–494, 2000.

K. Iwama, A. Matsuura, and M. Paterson.
A family of NFAs which need $2^n - \alpha$ deterministic states.
Theoret. Comput. Sci., 301(1-3):451–462, 2003.

G. Jirásková.
Deterministic blow-ups of minimal NFA's.
RAIRO Theor. Informatics Appl., 40(3):485–499, 2006.

References IV

G. Jirásková.

On the state complexity of complements, stars, and reversals of regular languages.
In Developments in Language Theory, 12th International Conference, DLT 2008, Kyoto, Japan, September 16-19, 2008. Proceedings, volume 5257 of Lecture Notes in Computer Science, pages 431–442. Springer, 2008.

G. Jirásková.

Magic numbers and ternary alphabet.
Int. J. Found. Comput. Sci., 22(2):331–344, 2011.

R. Koo.

A classification of matrices of finite order over $\mathbb{C}$, $\mathbb{R}$ and $\mathbb{Q}$.
Mathematics Magazine, 76(2):143–148, 2003.

R. Lidl and H. Niederreiter.

Finite fields, volume 20 of Encyclopedia of Mathematics and its Applications.
Cambridge University Press, Cambridge, second edition, 1997.
With a foreword by P. M. Cohn.

V. Marsault.

An efficient algorithm to decide periodicity of b-recognisable sets using LSDF convention.
Log. Methods Comput. Sci., 15(3), 2019.

A. R. Meyer and M. J. Fischer.

Economy of description by automata, grammars, and formal systems.
In 12th Annual Symposium on Switching and Automata Theory, East Lansing, Michigan, USA, October 13-15, 1971, pages 188–191. IEEE Computer Society, 1971.

References V

L. Mérai and A. Winterhof.
On the nth linear complexity of automatic sequences.
Journal of Number Theory, 187:415–429, 2018.

J. Ouaknine and J. Worrell.
Decision problems for linear recurrence sequences.
In RP 2012, volume 7550 of Lecture Notes in Computer Science, pages 21–28. Springer, 2012.

M. Rigo.
Mathématiques discrètes, notes de cours 2009–2010.
Available at http://www.discmath.ulg.ac.be/cours/main_sd.pdf.

J. O. Shallit and M. Wang.
Automatic complexity of strings.
J. Autom. Lang. Comb., 6(4):537–554, 2001.

N. J. A. Sloane.
The On-Line Encyclopedia of Integer Sequences.
http://oeis.org.

K. Sutner.
Divisibility and state complexity.
The Mathematica Journal, 11(3):430–445, 2009.

K. Sutner and S. Tetruashvili.
Inferring automatic sequences.
https://www.cs.cmu.edu/ sutner/papers/auto-seq.pdf, 2012.

References VI

M. Ward.

The arithmetical theory of linear recurring series.
Transactions of the American Mathematical Society, 35(3):600–628, 1933.

H. Zantema and W. Bosma.

Complexity of automatic sequences.
Information and Computation, 288:104710, 2022.
Special Issue: Selected Papers of the 14th International Conference on Language and Automata Theory and Applications, LATA 2020.