Arithmetics on Suffix Arrays of Fibonacci Words

Tomohiro I *Dominik Köppl*

Department of Computer Science, TU Dortmund, Germany

WORDS 2015

Fibonacci Words

$$F_n = \begin{cases} b & \text{if } n = 1, \\ a & \text{if } n = 2, \\ F_{n-1}F_{n-2} & \text{otherwise.} \end{cases}$$

- $F_3 = \texttt{ab}$
- $F_4 = \texttt{aba}$
- $F_5 = \texttt{abaab}$
- $F_6 = \texttt{abaababa}$

- $|F_n| = f_n$

Fibonacci Numbers

$$f_n = \begin{cases} 1 & \text{if } n = 1, \\ 1 & \text{if } n = 2, \\ f_{n-1} + f_{n-2} & \text{otherwise.} \end{cases}$$

- $f_3 = 2$
- $f_4 = 3$
- $f_5 = 5$
- $f_6 = 8$

suffix arrays

SA_5: suffix array of F_5:

- take suffixes of F_5
- sort them
- suffix array SA_5 is first column

$F_5 =$ abaab

1	a	b	a	a	b
2	b	a	a	b	
3	a	a	b		
4	a	b			
5	b				

suffix arrays

SA_5: suffix array of F_5:

- take suffixes of F_5
- sort them
- suffix array SA_5 is first column

$F_5 =$ abaab

3	a	a	b		
4	a	b			
1	a	b	a	a	b
5	b				
2	b	a	a	b	

suffix arrays

SA_5: suffix array of F_5:

- take suffixes of F_5
- sort them
- suffix array SA_5 is first column

$F_5 = \texttt{abaab}$

$\mathsf{SA}_5 = \texttt{3 4 1 5 2}$

SA_5					
3	a	a	b		
4	a	b			
1	a	b	a	a	b
5	b				
2	b	a	a	b	

BWT

BWT_5: Burrows Wheeler Transformation of $F_5 = \texttt{abaab}$

- same table as before
- first column: char before suffix
- first column = BWT_5 = babaa

3	a	a	b		
4	a	b			
1	a	b	a	a	b
5	b				
2	b	a	a	b	

BWT

BWT_5: Burrows Wheeler Transformation of $F_5 =$ `abaab`

- same table as before
- first column: char before suffix
- first column $= BWT_5 =$ `babaa`

b	3	a	a	b		
a	4	a	b			
b	1	a	b	a	a	b
a	5	b				
a	2	b	a	a	b	

BWT

BWT_5: Burrows Wheeler Transformation of $F_5 =$ `abaab`

- same table as before
- first column: char before suffix
- first column $= BWT_5 =$ `babaa`

b	3	a	a	b		
a	4	a	b			
b	1	a	b	a	a	b
a	5	b				
a	2	b	a	a	b	

F_6

i	1	2	3	4	5	6	7	8
F_6	a	b	a	a	b	a	b	a
SA_6	8	3	6	1	4	7	2	5
BWT_6	b	b	b	a	a	a	a	a

SA_6: suffix array, BWT_6: Burrows-Wheeler Transformation

F_6

i	1	2	3	4	5	6	7	8
F_6	a	b	a	a	b	a	b	a
SA_6	8	3	6	1	4	7	2	5
BWT_6	b	b	b	a	a	a	a	a

SA_6: suffix array, BWT_6: Burrows-Wheeler Transformation

Observations

- $\mathrm{BWT}_n = b^{f_4} a^{f_5}$ $(f_4 = 3, f_5 = 5)$

F_6

i	1	2	3	4	5	6	7	8
F_6	a	b	a	a	b	a	b	a
SA_6	8	3	6	1	4	7	2	5
BWT_6	b	b	b	a	a	a	a	a

SA_6: suffix array, BWT_6: Burrows-Wheeler Transformation

Observations

- $BWT_n = b^{f_4} a^{f_5}$ $\quad (f_4 = 3, f_5 = 5)$
- $SA_n[i] = SA_n[i-1] + f_4 \mod f_6$

F_6

i	1	2	3	4	5	6	7	8
F_6	a	b	a	a	b	a	b	a
SA_6	8	3	6	1	4	7	2	5
BWT_6	b	b	b	a	a	a	a	a

SA_6: suffix array, BWT_6: Burrows-Wheeler Transformation

Observations

- $BWT_n = b^{f_4} a^{f_5}$ $\quad (f_4 = 3, f_5 = 5)$
- $SA_n[i] = SA_n[i-1] + f_4 \mod f_6$

Definition

SA_n is called ***arithmetically progressed*** if $\exists k \in \mathbb{N}$:

$$SA_n[i] = SA_n[i-1] + k \mod |SA_n| \; \forall i$$

works for *all* fibos?

Conjecture

SA_n is arithmetically progressed for every n.

works for *all* fibos?

Conjecture

SA_n is arithmetically progressed for every n.

Does not hold!

i	1	2	3	4	5
F_5	a	b	a	a	b
SA_5	3	4	1	5	2

our results

- SA_n is arithmetically progressed for *even n*
- $\mathrm{BWT}_n = \mathtt{b}^{f_{n-2}}\mathtt{a}^{f_{n-1}}$ for *even n*

our results

- SA_n is arithmetically progressed for *even n*
- $\mathrm{BWT}_n = \mathtt{b}^{f_{n-2}}\mathtt{a}^{f_{n-1}}$ for *even n*

Wait a sec! What about

Theorem (Mantaci et al'03)
$\mathrm{BWT}_n = b^{f_{n-2}}a^{f_{n-1}}$ *for all n.*

our results

- SA_n is arithmetically progressed for *even n*
- $\mathrm{BWT}_n = \mathtt{b}^{f_{n-2}}\mathtt{a}^{f_{n-1}}$ for *even n*

Wait a sec! What about

Theorem (Mantaci et al'03)
$\mathrm{BWT}_n = b^{f_{n-2}}a^{f_{n-1}}$ *for all n.*

We look at suffix based BWT, not rotation based BWT!

$\mathrm{BWT}_{F_5\$}$

$F_5\$ = abaab\$$

by rotation

a	b	a	a	b	$
$	a	b	a	a	b
b	$	a	b	a	a
a	b	$	a	b	a
a	a	b	$	a	b
b	a	a	b	$	a
F					*L*

by suffixes

$	a	b	a	a	b	$
a	b	a	a	b	$	
b	a	a	b	$		
a	a	b	$			
a	b	$				
b	$					
-1						

$\mathrm{BWT}_{F_5\$}$ $\quad F_5\$ = abaab\$$

by rotation

$	a	b	a	a	b
a	a	b	$	a	b
a	b	$	a	b	a
a	b	a	a	b	$
b	$	a	b	a	a
b	a	a	b	$	a
F					*L*

$\mathrm{BWT}_{\texttt{abaab\$}} = \texttt{bba\$aa}$

by suffixes

$	a	b	a	a	b	$
a	b	a	a	b	$	
b	a	a	b	$		
a	a	b	$			
a	b	$				
b	$					
-1						

$BWT_{F_5\$}$ $F_5\$ = abaab\$$

by rotation

$	a	b	a	a	b
a	a	b	$	a	b
a	b	$	a	b	a
a	b	a	a	b	$
b	$	a	b	a	a
b	a	a	b	$	a
F					*L*

$BWT_{\texttt{abaab\$}} = \texttt{bba\$aa}$

by suffixes

$	a	b	a	a	b	$
a	b	a	a	b	$	
b	a	a	b	$		
a	a	b	$			
a	b	$				
b	$					
-1						

$\mathrm{BWT}_{F_5\$}$

$F_5\$ = abaab\$$

by rotation

$	a	b	a	a	b
a	a	b	$	a	b
a	b	$	a	b	a
a	b	a	a	b	$
b	$	a	b	a	a
b	a	a	b	$	a
F					*L*

$\mathrm{BWT}_{\texttt{abaab\$}} = \mathrm{bba\$aa}$

by suffixes

b	$					
b	a	a	b	$		
a	a	b	$			
$	a	b	a	a	b	$
a	b	$				
a	b	a	a	b	$	
-1						

$\mathrm{BWT}_{\texttt{abaab\$}} = \mathrm{bba\$aa}$

BWT_{F_5} $\quad F_5 = abaab$

by rotation

a	b	a	a	b
b	a	b	a	a
a	b	a	b	a
a	a	b	a	b
b	a	a	b	a
F				L

by suffixes

b	a	b	a	a	b
a	b	a	a	b	
b	a	a	b		
a	a	b			
a	b				
-1					

BWT_{F_5} $\quad F_5 = abaab$

by rotation

a	a	b	a	b
a	b	a	a	b
a	b	a	b	a
b	a	a	b	a
b	a	b	a	a
F				*L*

by suffixes

b	a	b	a	a	b
a	b	a	a	b	
b	a	a	b		
a	a	b			
a	b				
-1					

$\mathrm{BWT}_{\texttt{abaab}} = \texttt{bbaaa}$

BWT_{F_5} $\quad F_5 = abaab$

by rotation

a	a	b	a	b
a	b	a	a	b
a	b	a	b	a
b	a	a	b	a
b	a	b	a	a
F				L

$\mathrm{BWT}_{\texttt{abaab}} = \texttt{bbaaa}$

by suffixes

b	a	a	b		
a	a	b			
b	a	b	a	a	b
a	b				
a	b	a	a	b	
-1					

$\mathrm{BWT}_{\texttt{abaab}} = \texttt{babaa}$

Without \$ both variants *differ*!

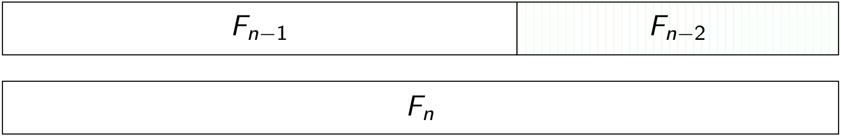
let's start. . .

splits for n even

F_n

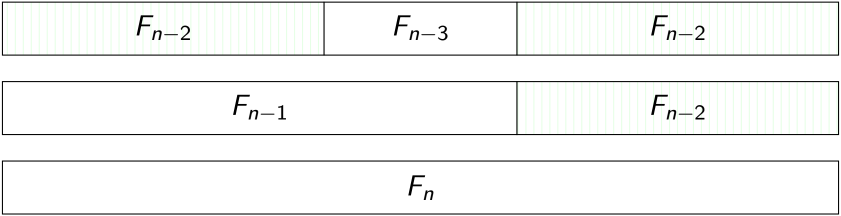
splits for n even

- $F_n = F_{n-1}F_{n-2}$



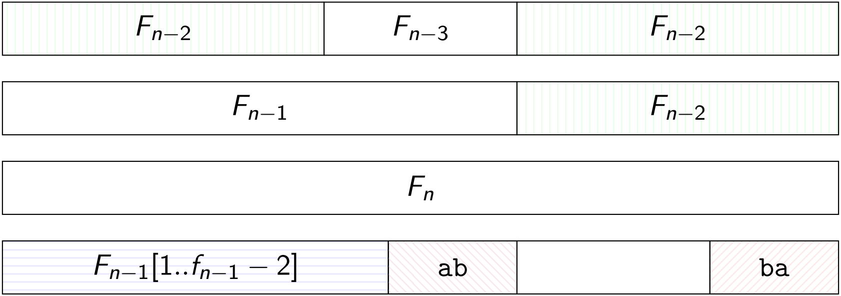
splits for n even

- $F_n = F_{n-1}F_{n-2}$
- $F_{n-1} = F_{n-2}F_{n-3}$



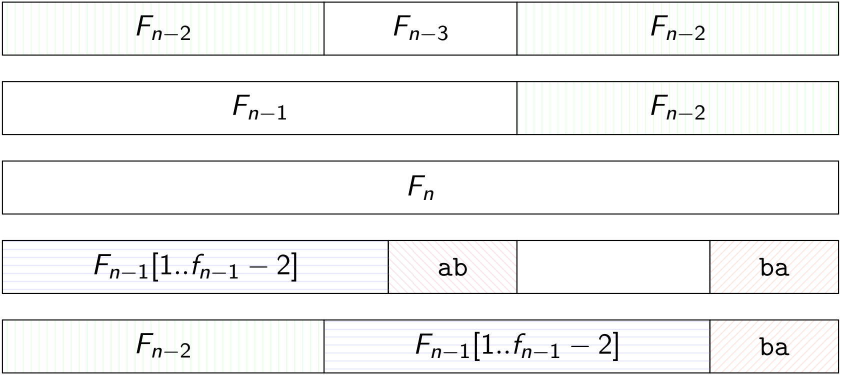
splits for n even

- $F_n = F_{n-1}F_{n-2}$
- $F_{n-1} = F_{n-2}F_{n-3}$
- $F_n = \ldots\texttt{ba}$ and $F_{n-1} = \ldots\texttt{ab}$ [induction]



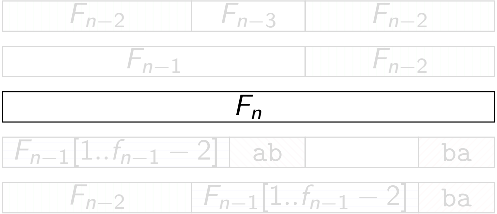
splits for n even

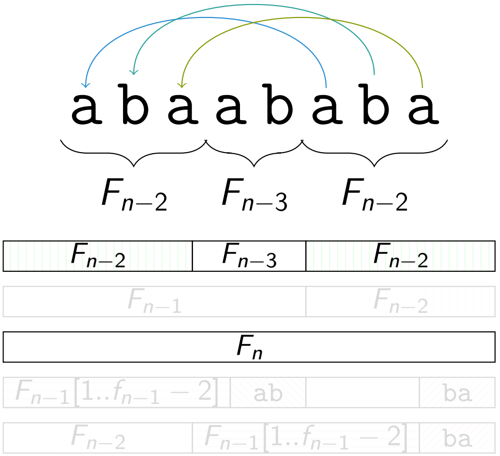
- $F_n = F_{n-1}F_{n-2}$
- $F_{n-1} = F_{n-2}F_{n-3}$
- $F_n = \ldots\texttt{ba}$ and $F_{n-1} = \ldots\texttt{ab}$ [induction]
- $F_n = F_{n-2}F_{n-1}[1..f_{n-1} - 2]\texttt{ba}$ [Christodoulakis et al'03]

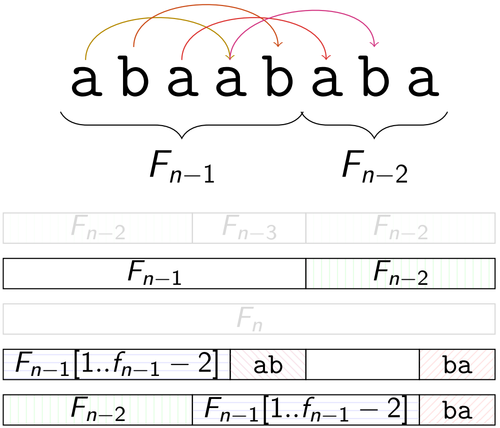


SA_n is arithmetically progressed

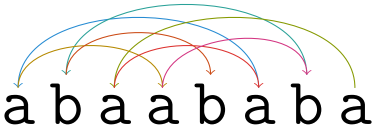
a b a a b a b a




a b a a b a b a
F_{n-2}
F_{n-3}
F_{n-2}
F_{n-2} | F_{n-3} | F_{n-2}
F_{n-1} | F_{n-2}
F_n
$F_{n-1}[1..f_{n-1}-2]$ | ab | | ba
F_{n-2} | $F_{n-1}[1..f_{n-1}-2]$ | ba

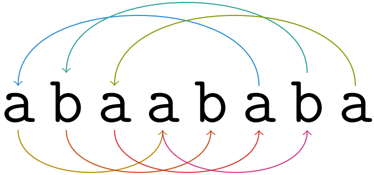


a b a a b a b a
F_{n-1}
F_{n-2}
F_{n-2}
F_{n-3}
F_{n-2}
F_{n-1}
F_{n-2}
F_n
$F_{n-1}[1..f_{n-1}-2]$
ab
ba
F_{n-2}
$F_{n-1}[1..f_{n-1}-2]$
ba


a b a a b a b a

moves:

$SA_6 = 8$



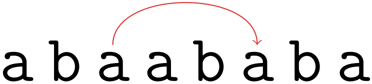
moves: -5

$\mathsf{SA}_6 =$ 8 3

a b a a b a b a

moves: -5 $+3$

$\mathsf{SA}_6 =$ 8 3 6



moves: $-5 \;\; +3 \;\; -5$

$SA_6 = \;\; 8 \; 3 \; 6 \; 1$

a b a a b a b a

moves: $-5 \quad +3 \quad -5 \quad +3$

$\mathsf{SA}_6 = \; 8 \; 3 \; 6 \; 1 \; 4$

a b a a b a b a

moves: -5 $+3$ -5 $+3$ $+3$

$SA_6 =$ 8 3 6 1 4 7

a b a a b a b a

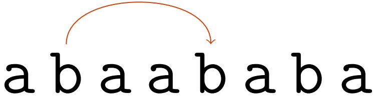
moves: -5 $+3$ -5 $+3$ $+3$ -5

$SA_6 =$ 8 3 6 1 4 7 2

a b a a b a b a

moves: -5 $+3$ -5 $+3$ $+3$ -5 $+3$

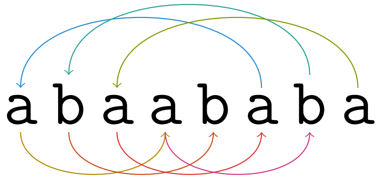
$\mathsf{SA}_6 =$ 8 3 6 1 4 7 2 5



moves: -5 $+3$ -5 $+3$ $+3$ -5 $+3$

$SA_6 =$ 8 3 6 1 4 7 2 5

We move always $3 \mod f_6$ **right!**



main result

for n even:

Theorem

$$\mathsf{SA}_n[i] = \begin{cases} f_n & \text{if } i = 1, \\ (\mathsf{SA}_n[i-1] + f_{n-2}) \mod f_n & \text{otherwise.} \end{cases}$$

$$\mathsf{BWT}_n = \mathtt{b}^{f_{n-2}}\mathtt{a}^{f_{n-1}}$$

2-letter substrings of F_n

Running example F_6:

i	1	2	3	4	5	6	7	8
F_6	a	b	a	a	b	a	b	a
SA_6	8	3	6	1	4	7	2	5
$F_6[\mathrm{SA}_n[i]]$	a	a	a	a	a	b	b	b
BWT_6	b	b	b	a	a	a	a	a

2-letter substrings of F_n

Running example F_6:

i	1	2	3	4	5	6	7	8
F_6	a	b	a	a	b	a	b	a
SA_6	8	3	6	1	4	7	2	5
$F_6[\mathsf{SA}_n[i]]$	a	a	a	a	a	b	b	b
BWT_6	b	b	b	a	a	a	a	a

Observation

$F_n[\mathsf{SA}_n[i]-1]$	b $\cdots$ b	a $\cdots$ a	a $\cdots$ a
$F_n[\mathsf{SA}_n[i]]$	a $\cdots$ a	a $\cdots$ a	b $\cdots$ b
Blocks	ba-type	aa-type	ab-type

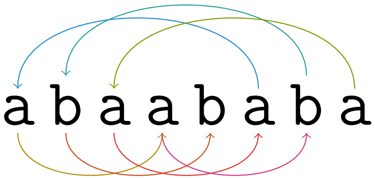
BWT_6

- $\mathrm{BWT}_n[i] = F_n[\mathrm{SA}_n[i] - 1]$

a b a a b a b a

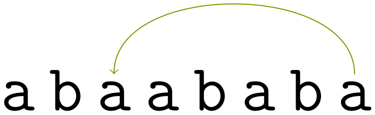
BWT$_6$

- $\mathrm{BWT}_n[i] = F_n[\mathrm{SA}_n[i] - 1]$
- follow SA_n-arrows



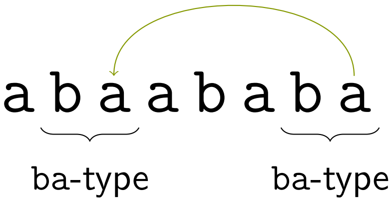
$\mathsf{BWT}_6 = \mathtt{b}$

- $\mathsf{BWT}_n[i] = F_n[\mathsf{SA}_n[i] - 1]$
- follow SA_n-arrows
- start at $\mathsf{SA}_n[1] = f_n$



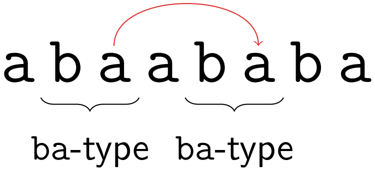
$\mathrm{BWT}_6 = \texttt{b b}$

- $\mathrm{BWT}_n[i] = F_n[\mathrm{SA}_n[i] - 1]$
- follow SA_n-arrows
- start at $\mathrm{SA}_n[1] = f_n$



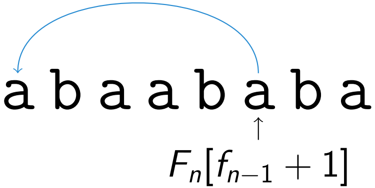
$\mathrm{BWT}_6 = \mathtt{b\ b\ b}$

- $\mathrm{BWT}_n[i] = F_n[\mathrm{SA}_n[i] - 1]$
- follow SA_n-arrows
- start at $\mathrm{SA}_n[1] = f_n$



$\mathrm{BWT}_6 = \mathtt{b\ b\ b\ a}$

- $\mathrm{BWT}_n[i] = F_n[\mathrm{SA}_n[i] - 1]$
- follow SA_n-arrows
- start at $\mathrm{SA}_n[1] = f_n$



$\mathsf{BWT}_6 = \mathtt{b\ b\ b\ a} \cdots \mathtt{a}$

- $\mathsf{BWT}_n[i] = F_n[\mathsf{SA}_n[i] - 1]$
- follow SA_n-arrows
- start at $\mathsf{SA}_n[1] = f_n$

$$\mathtt{a\ b\ a\ a\ b\ a\ b\ a}$$

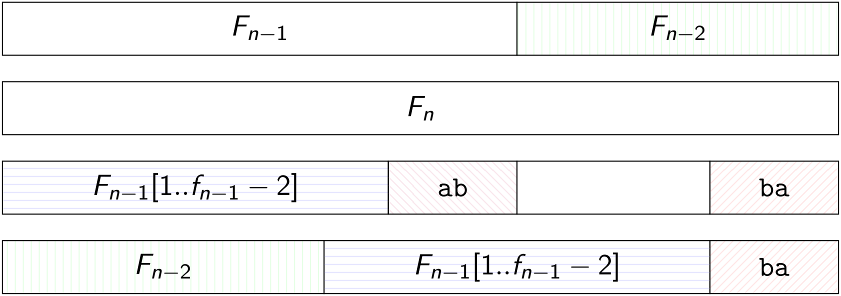
$$\uparrow$$

$$F_n[f_{n-1} + 1]$$

Proposition

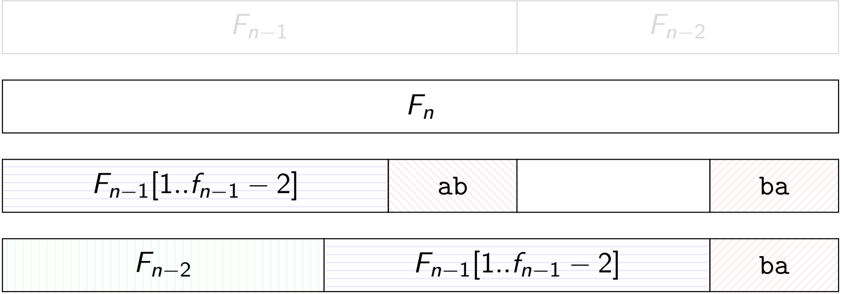
The run of ba-types ends at suffix $F_n[f_{n-1} + 1..]$ $(f_5 = 5)$

splits



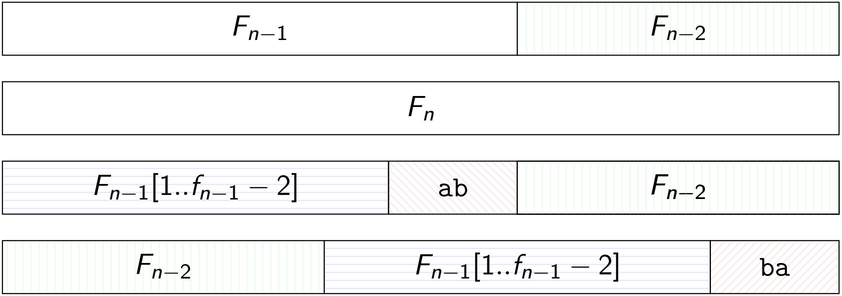
- $F_n[i] = F_n[i + f_{n-2}]\ \forall\, i = 1, \dots, f_{n-1} - 2$
- $F_n[i] = F_n[i + f_{n-1}]\ \forall\, i = 1, \dots, f_{n-2}$
- Move $f_{n-2} \mod f_n$ chars right $\Rightarrow$ find same 2-letter substring! (not true at $F_n[f_{n-1} - 1..f_{n-1}]$.)

splits



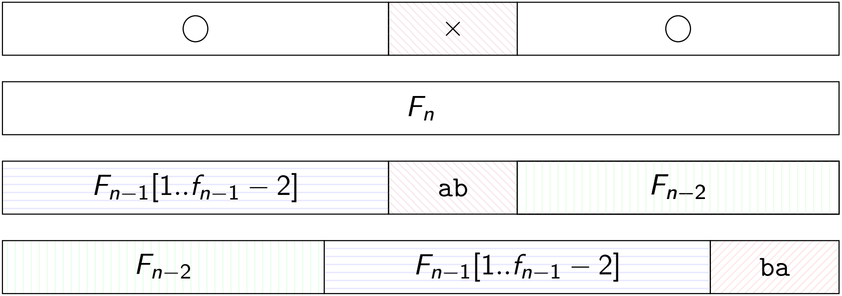
- $F_n[i] = F_n[i + f_{n-2}]\ \forall\, i = 1, \ldots, f_{n-1} - 2$
- $F_n[i] = F_n[i + f_{n-1}]\ \forall\, i = 1, \ldots, f_{n-2}$
- Move $f_{n-2} \mod f_n$ chars right $\Rightarrow$ find same 2-letter substring! (not true at $F_n[f_{n-1} - 1..f_{n-1}]$.)

splits



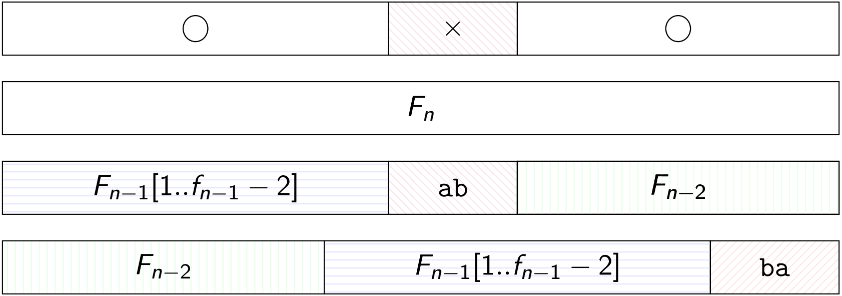
- $F_n[i] = F_n[i + f_{n-2}] \; \forall\, i = 1, \ldots, f_{n-1} - 2$
- $F_n[i] = F_n[i + f_{n-1}] \; \forall\, i = 1, \ldots, f_{n-2}$
- Move $f_{n-2} \mod f_n$ chars right $\Rightarrow$ find same 2-letter substring! (not true at $F_n[f_{n-1} - 1..f_{n-1}]$.)

splits



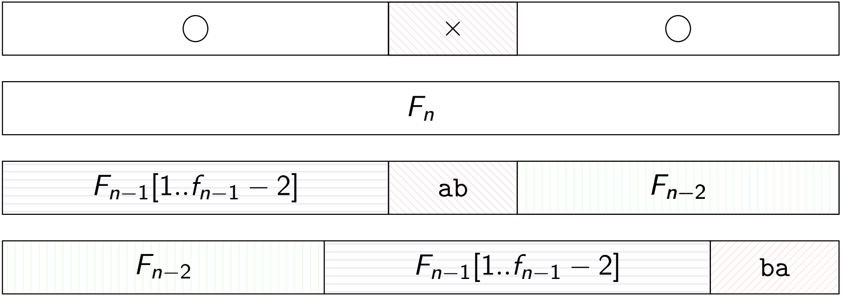
- $F_n[i] = F_n[i + f_{n-2}] \; \forall \, i = 1, \ldots, f_{n-1} - 2$
- $F_n[i] = F_n[i + f_{n-1}] \; \forall \, i = 1, \ldots, f_{n-2}$
- Move $f_{n-2} \mod f_n$ chars right $\Rightarrow$ find same 2-letter substring! (not true at $F_n[f_{n-1} - 1..f_{n-1}]$.)

hunting ba-types



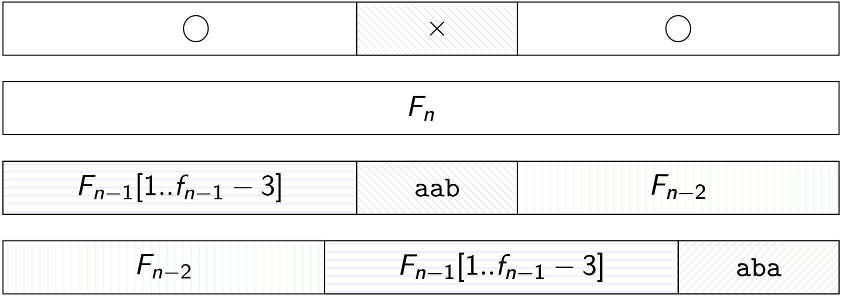
- $\mathrm{SA}_n[1] = f_n$ and $F_n[f_n - 1..] = ba$
- find ba-types until reaching $\times$
- SA_n arithmetically progressed, step f_{n-2} [proved]
- $\mathrm{SA}_n[f_{n-2}] = f_{n-1} + 1$ [calculate]

hunting ba-types



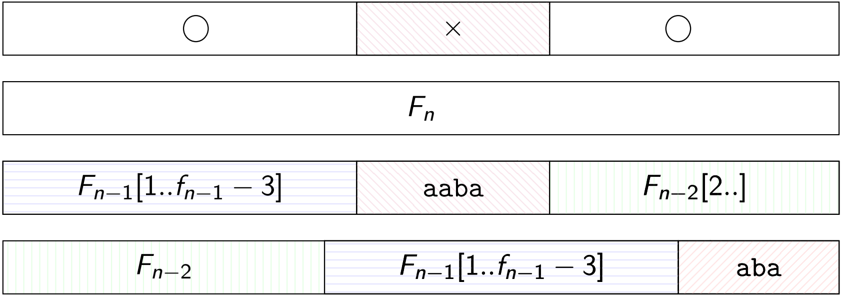
- $SA_n[1] = f_n$ and $F_n[f_n - 1..] = ba$
- find ba-types until reaching $\times$
- SA_n arithmetically progressed, step f_{n-2} [proved]
- $SA_n[f_{n-2}] = f_{n-1} + 1$ [calculate]

hunting ba-types



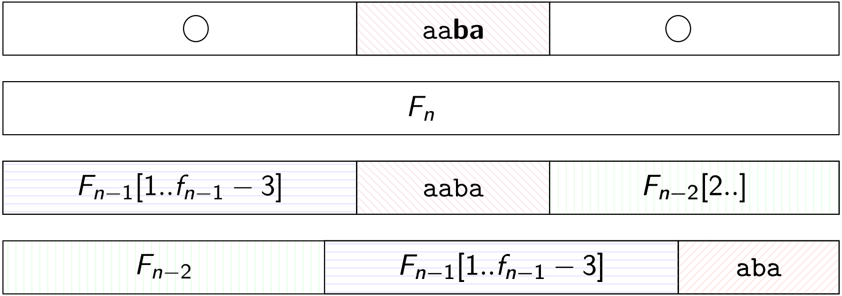
- $\mathrm{SA}_n[1] = f_n$ and $F_n[f_n - 1..] = ba$
- find ba-types until reaching $\times$
- SA_n arithmetically progressed, step f_{n-2} [proved]
- $\mathrm{SA}_n[f_{n-2}] = f_{n-1} + 1$ [calculate]

hunting ba-types



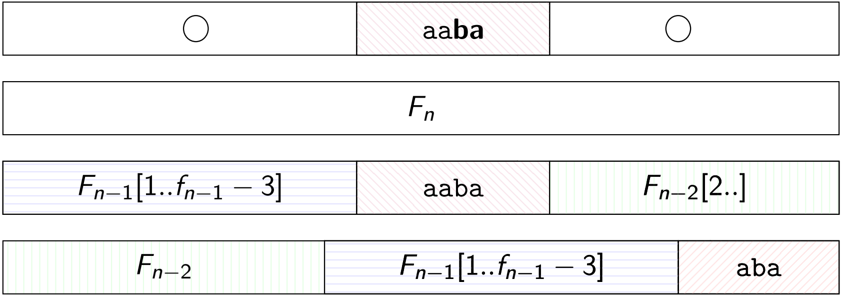
- $\mathrm{SA}_n[1] = f_n$ and $F_n[f_n - 1..] = ba$
- find ba-types until reaching $\times$
- SA_n arithmetically progressed, step f_{n-2} [proved]
- $\mathrm{SA}_n[f_{n-2}] = f_{n-1} + 1$ [calculate]

hunting ba-types



- $\mathrm{SA}_n[1] = f_n$ and $F_n[f_n - 1..] = ba$
- find ba-types until reaching $\times$
- SA_n arithmetically progressed, step f_{n-2} [proved]
- $\mathrm{SA}_n[f_{n-2}] = f_{n-1} + 1$ [calculate]

hunting ba-types



- $\mathsf{SA}_n[1] = f_n$ and $F_n[f_n - 1..] = ba$
- find ba-types until reaching $\times$
- SA_n arithmetically progressed, step f_{n-2} [proved]
- $\mathsf{SA}_n[f_{n-2}] = f_{n-1} + 1$ [calculate]

Theorem

$\mathrm{BWT}_n = b^{f_{n-2}} a^{f_{n-1}}$ *for even n.*

- $\#\mathtt{b} = f_{n-2}$ [folklore]
- $\mathrm{SA}_n[f_{n-2}] = f_{n-1} + 1$ [previous slide]
- Found all ba-substrings! □

summary

results

- SA_n arithmetically progressed for *even n*
- BWT_n based on suffixes $= \mathtt{b}^{f_{n-2}}\mathtt{a}^{f_{n-1}}$ for *even n*

further results (read the paper!)

- $\mathrm{SA}_n[i] = \mathrm{ISA}_{F_n}[i + f_{n-2} + 1 \mod f_n]$ for *even n*
- any LZ77 factor of F_n has same properties
- pre-/appending chars $\Rightarrow$ similar characteristics

open problems

- class of strings that has the same properties?
- what about odd n?

Thank you for listening. Any questions are welcome!

summary

results

- SA_n arithmetically progressed for *even* n
- BWT_n based on suffixes $= \mathtt{b}^{f_{n-2}}\mathtt{a}^{f_{n-1}}$ for *even* n

further results (read the paper!)

- $\mathsf{SA}_n[i] = \mathsf{ISA}_{F_n}[i + f_{n-2} + 1 \mod f_n]$ for *even* n
- any LZ77 factor of F_n has same properties
- pre-/appending chars $\Rightarrow$ similar characteristics

open problems

- class of strings that has the same properties?
- what about odd n?

Thank you for listening. Any questions are welcome!

F_6

i	1	2	3	4	5	6	7	8
F_6	a	b	a	a	b	a	b	a
SA_6	8	3	6	1	4	7	2	5
ISA_{F_6}	4	7	2	5	8	3	6	1

SA_n: suffix array, ISA: inverse suffix array

F_6

i	1	2	3	4	5	6	7	8
F_6	a	b	a	a	b	a	b	a
SA_6	8	3	6	1	4	7	2	5
ISA_{F_6}	4	7	2	5	8	3	6	1

SA_n: suffix array, ISA: inverse suffix array

Observation

- $SA_6[i + f_4 \mod f_6] = ISA_{F_6}[i]$ $\qquad (f_4 = 3)$

F_6

i	1	2	3	4	5	6	7	8
F_6	a	b	a	a	b	a	b	a
SA_6	8	3	6	1	4	7	2	5
ISA_{F_6}	4	7	2	5	8	3	6	1

SA_n: suffix array, ISA: inverse suffix array

Observation

- $SA_6[i + f_4 \mod f_6] = ISA_{F_6}[i]$ $\quad (f_4 = 3)$

Definition

ISA is called a rotation of $SA_n \Leftrightarrow \exists k \in \mathbb{N}$ (called shift):

$$SA_n[i] = ISA[(k + i) \mod |SA_n|]$$

rotation theorem

for n even:

$$\mathsf{SA}_n[i] = \begin{cases} f_n & \text{if } i = 1, \\ (\mathsf{SA}_n[i-1] + f_{n-2}) \mod f_n & \text{otherwise.} \end{cases}$$

rotation theorem

for n even:

$$\mathsf{SA}_n[i] = \begin{cases} f_n & \text{if } i = 1, \\ (\mathsf{SA}_n[i-1] + f_{n-2}) \mod f_n & \text{otherwise.} \end{cases}$$

- $f_{n-2}^2 \mod f_n = 1$ [Folklore]

rotation theorem

for n even:

$$\mathrm{SA}_n[i] = \begin{cases} f_n & \text{if } i = 1, \\ (\mathrm{SA}_n[i-1] + f_{n-2}) \mod f_n & \text{otherwise.} \end{cases}$$

- $f_{n-2}^2 \mod f_n = 1$ [Folklore]

ISA is a rotation of SA_n:

$$\begin{aligned} \mathrm{SA}_n[i + f_{n-2} \mod f_n] &= \mathrm{SA}_n[i] + f_{n-2}^2 \mod f_n \\ &= \mathrm{SA}_n[i] + 1 \mod f_n \end{aligned}$$

Hence:

$$\mathrm{ISA}[\mathrm{SA}_n[i] + 1 \mod f_n] = i + f_{n-2} \mod f_n$$

ISA **is arithmetically progressed like** SA_n**, so its a rotation of** SA_n**.**

rotation theorem

for n even:

$$\mathsf{SA}_n[i] = \begin{cases} f_n & \text{if } i = 1, \\ (\mathsf{SA}_n[i-1] + f_{n-2}) \mod f_n & \text{otherwise.} \end{cases}$$

- $\mathsf{SA}_n[1] = f_n$

rotation theorem

for n even:

$$\mathsf{SA}_n[i] = \begin{cases} f_n & \text{if } i = 1, \\ (\mathsf{SA}_n[i-1] + f_{n-2}) \mod f_n & \text{otherwise.} \end{cases}$$

- $\mathsf{SA}_n[1] = f_n$
- $\mathsf{SA}_n[f_n] = \mathsf{SA}_n[1] + (f_n - 1) f_{n-2} \mod f_n$ [by recursion]

rotation theorem

for n even:

$$\mathsf{SA}_n[i] = \begin{cases} f_n & \text{if } i = 1, \\ (\mathsf{SA}_n[i-1] + f_{n-2}) \mod f_n & \text{otherwise.} \end{cases}$$

- $\mathsf{SA}_n[1] = f_n$
- $\mathsf{SA}_n[f_n] = \mathsf{SA}_n[1] + (f_n - 1) f_{n-2} \mod f_n$ [by recursion]

shift is

$$\begin{aligned} \mathsf{SA}_n[f_n] - \mathsf{ISA}[f_n] \mod f_n &\equiv \mathsf{SA}_n[f_n] - \mathsf{ISA}[\mathsf{SA}_n[1]] \\ &\equiv \mathsf{SA}_n[f_n] - 1 \\ &\equiv f_n + (f_n - 1) f_{n-2} - 1 \\ &\equiv -f_{n-2} - 1 \\ &\quad (\text{treat } f_n \triangleq 0) \end{aligned}$$