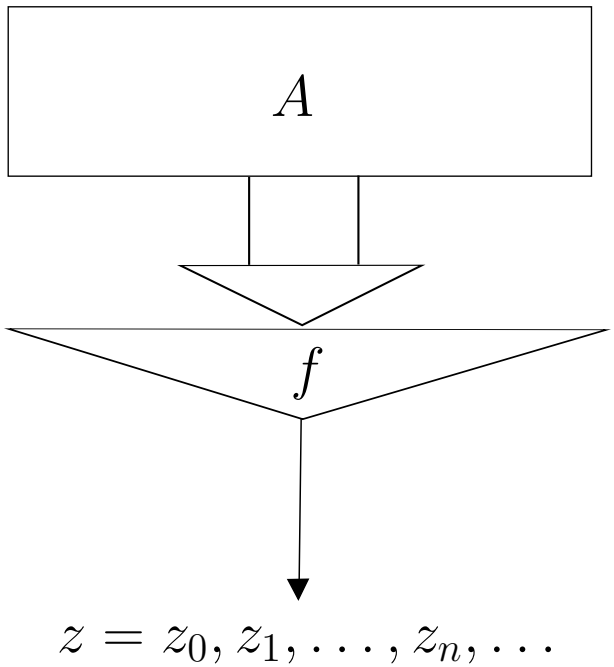
On the properties of Boolean functions related to planar approximation of the filter generator

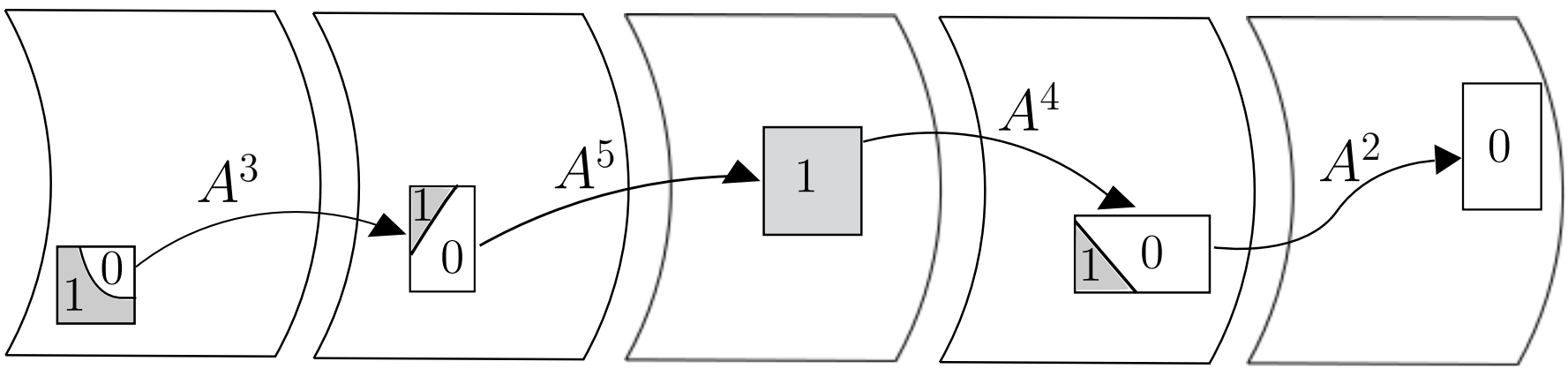
Alekseev E.K.[1], Kuschinskaya L.A.[2]

[1]CryptoPro LCC, [2]Lomonosov Moscow State University

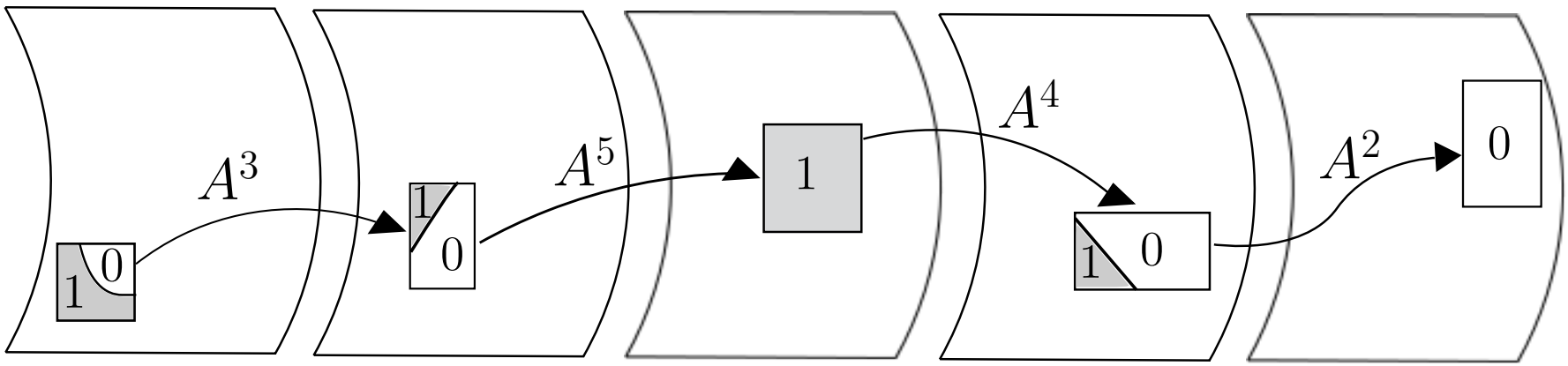
June 4, 2019



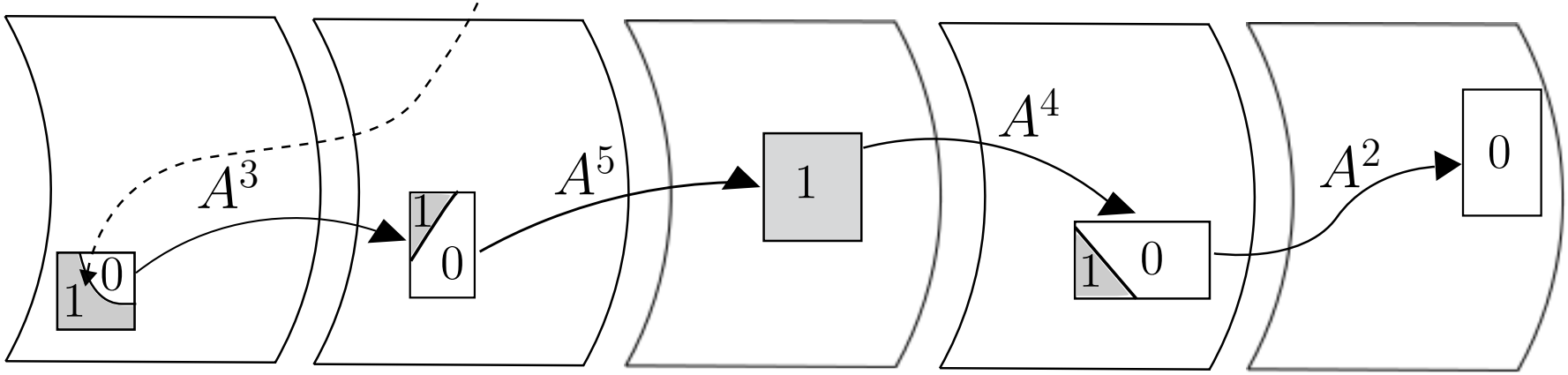
Filter generator is a construction built on the basis of linear mapping $A : V_n \to V_n$ and the Boolean function $f \in \mathcal{F}_n$.


A^3
A^5
A^4
A^2
1
0
1
0
1
1
0
0

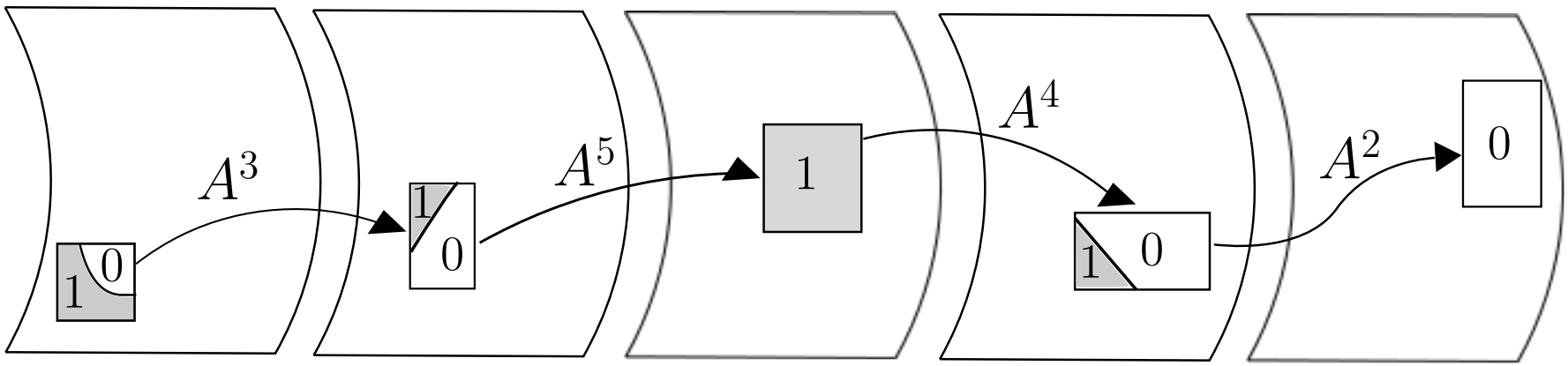
$$z = 00101100010110000...$$



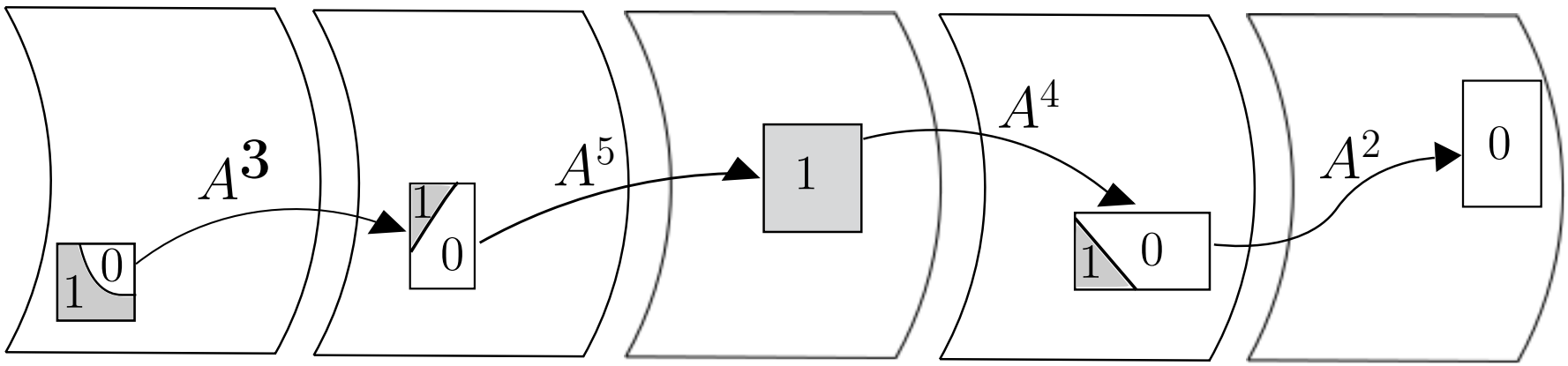
$$z = \mathbf{0}0101100010110000\ldots$$



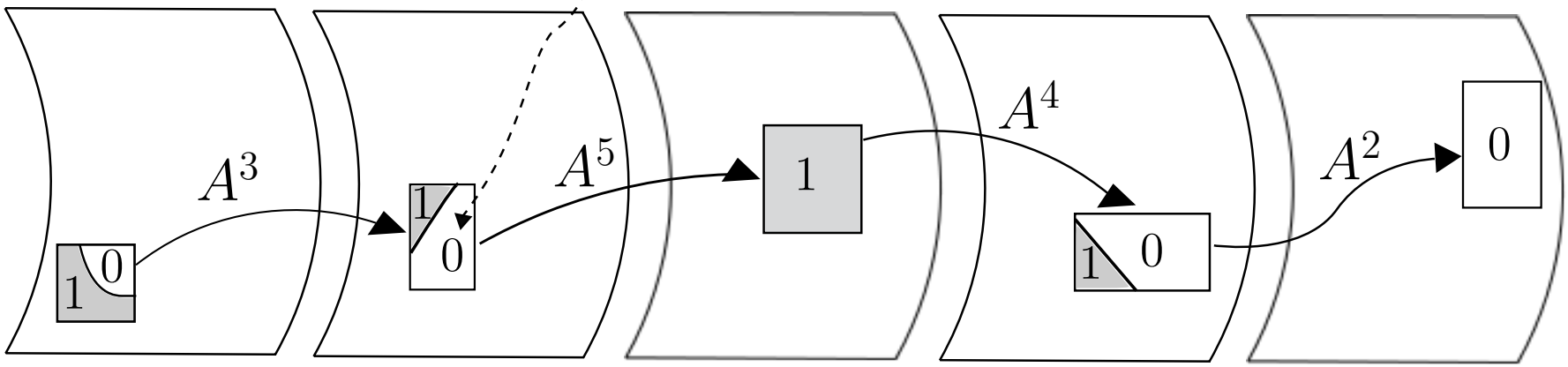
$$z = \underline{\mathbf{0}}0101100010110000...$$



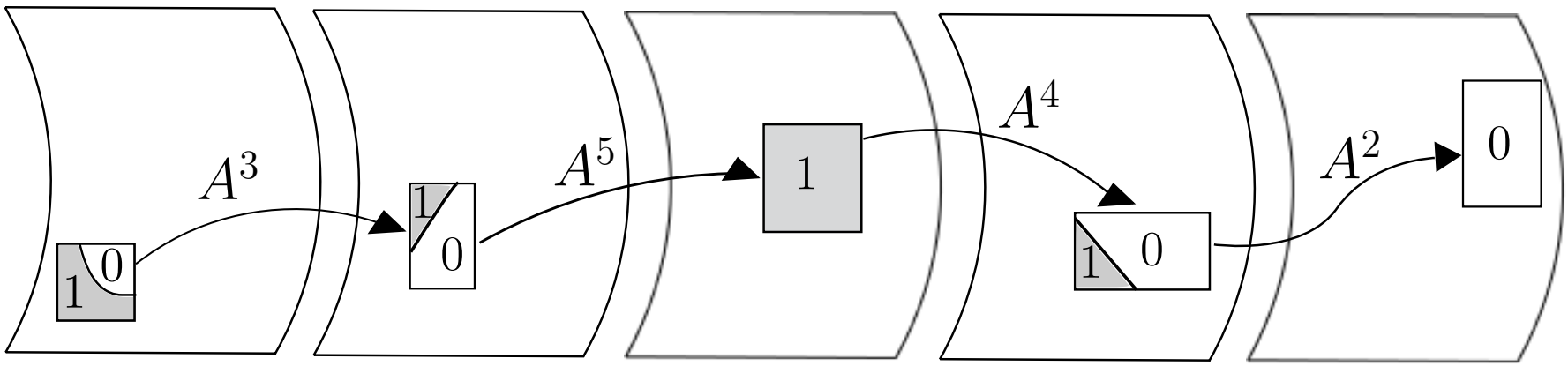
$$z = \overset{\overset{3}{\frown}}{\underline{0}0110110001011000 0}...$$

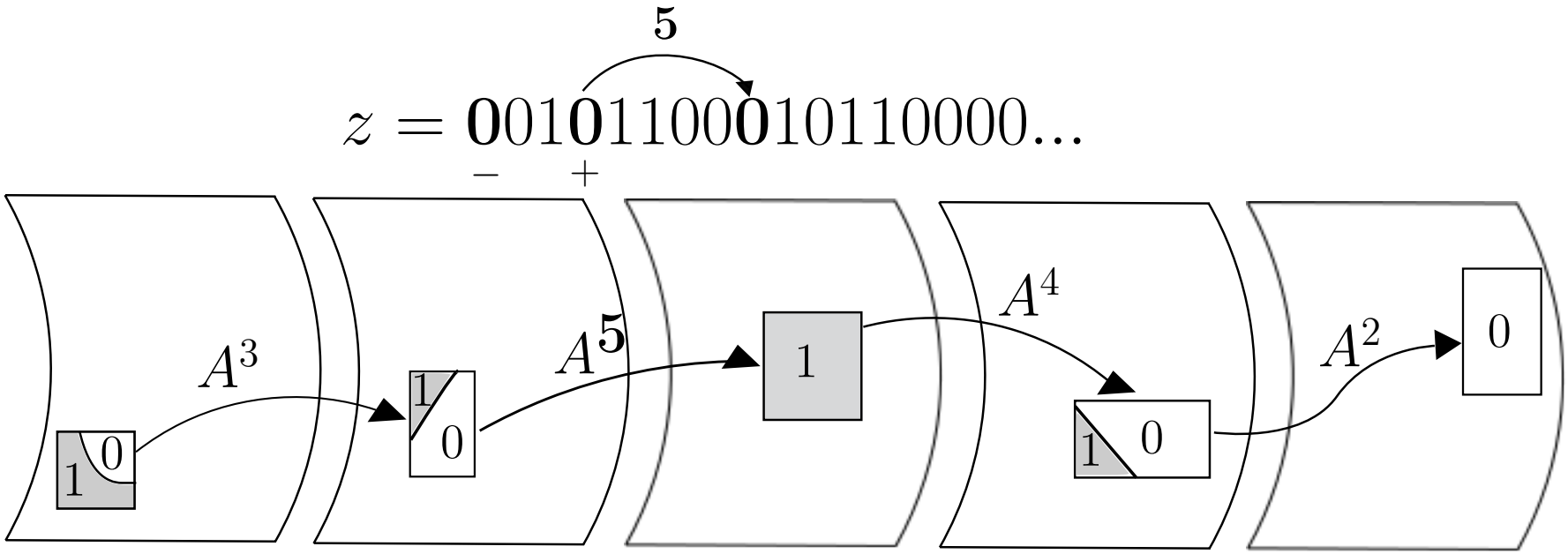


$$z = \underline{\mathbf{0}}01\underline{\mathbf{0}}1100010110000...$$

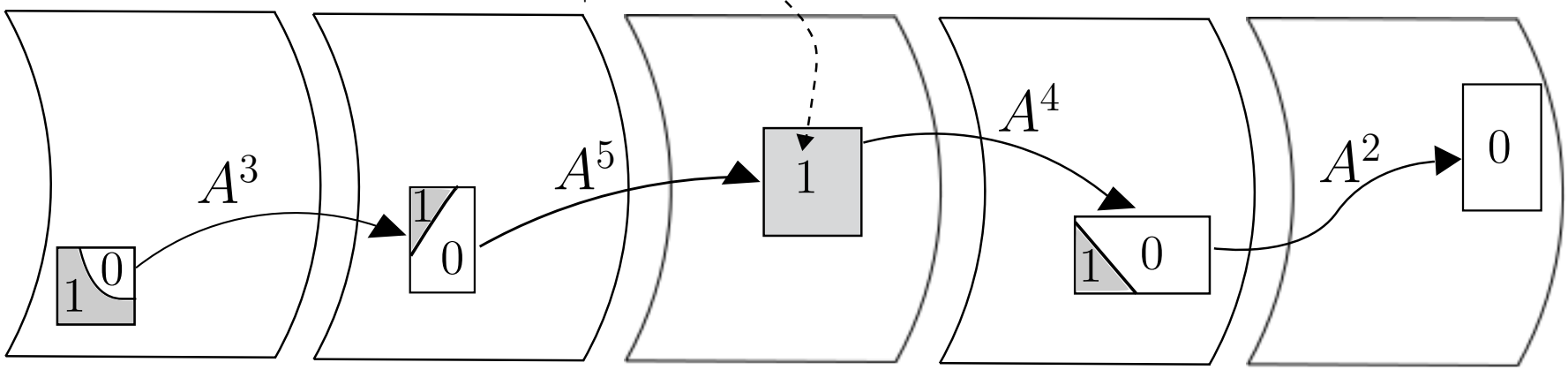


$$z = \underset{-}{\mathbf{0}}01\underset{+}{\mathbf{0}}1100010110000...$$

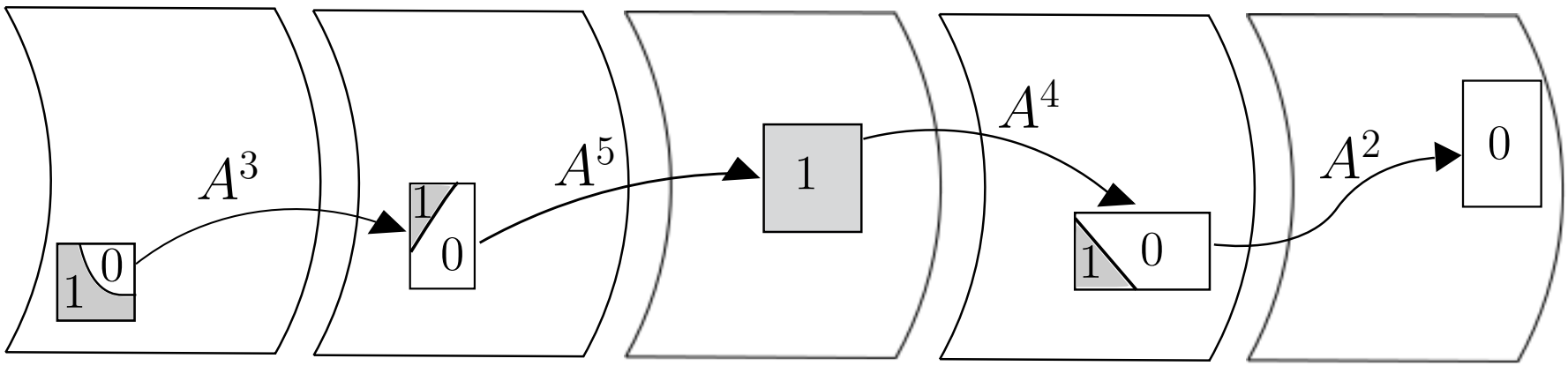


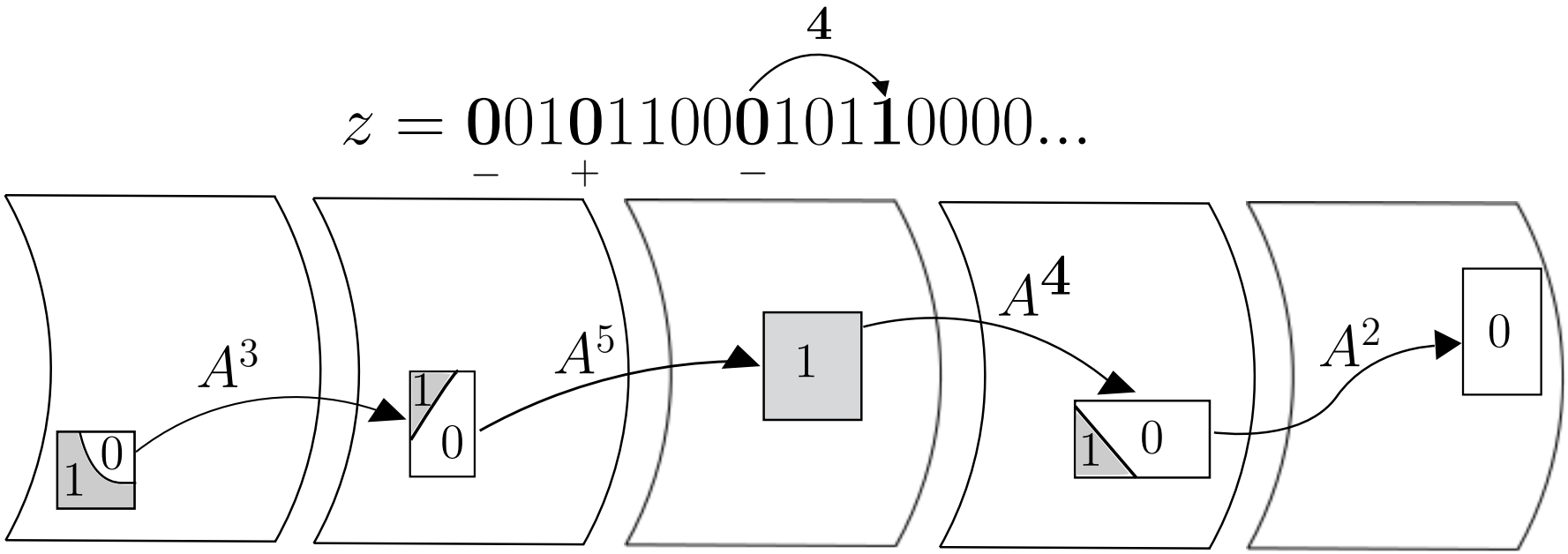

5
z = 0010110001011000...
− +
A^3
A^5
A^4
A^2
1
0
1
0
1
1
0
1
0
0

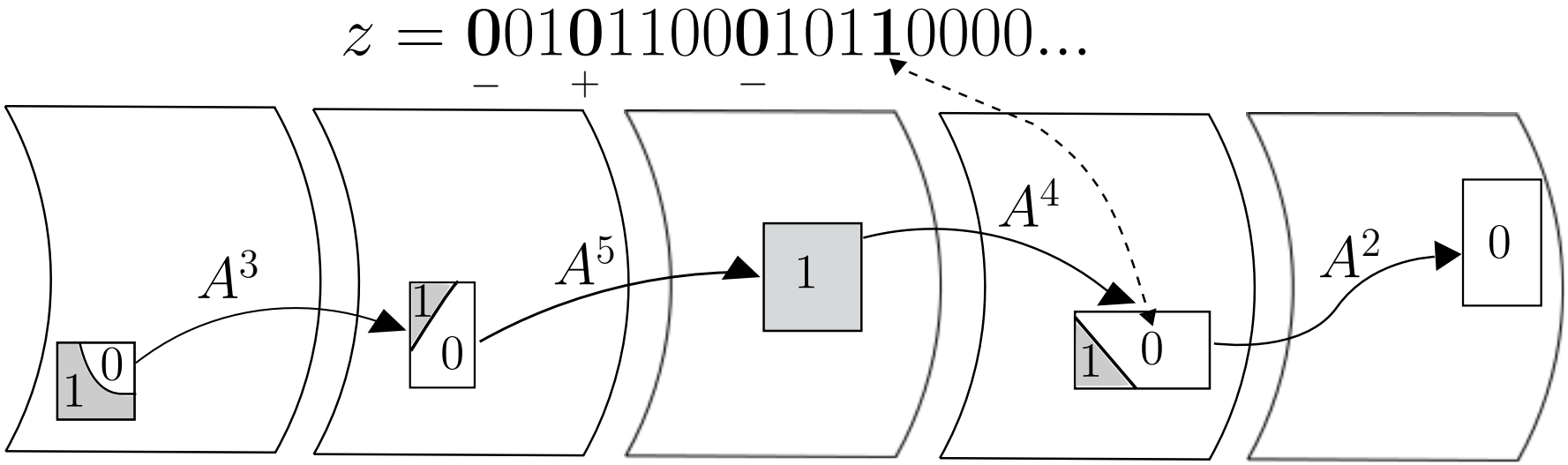
$$z = \mathbf{0}01\mathbf{0}1100\mathbf{0}10110000\ldots$$
$$\quad\; - \quad +$$



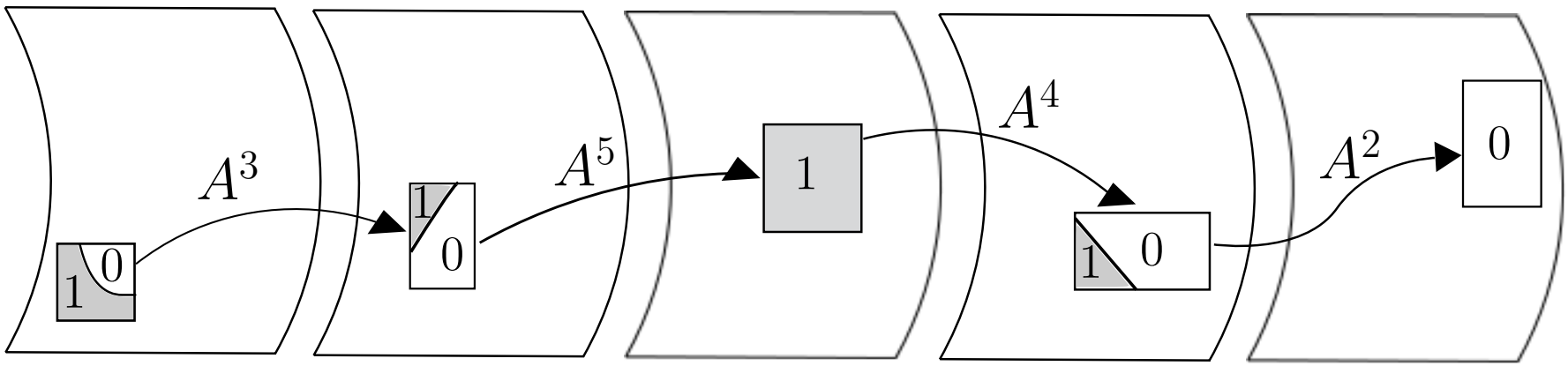
$$z = \underset{-}{\mathbf{0}}01\underset{+}{\mathbf{0}}1100\underset{-}{\mathbf{0}}10110000\ldots$$

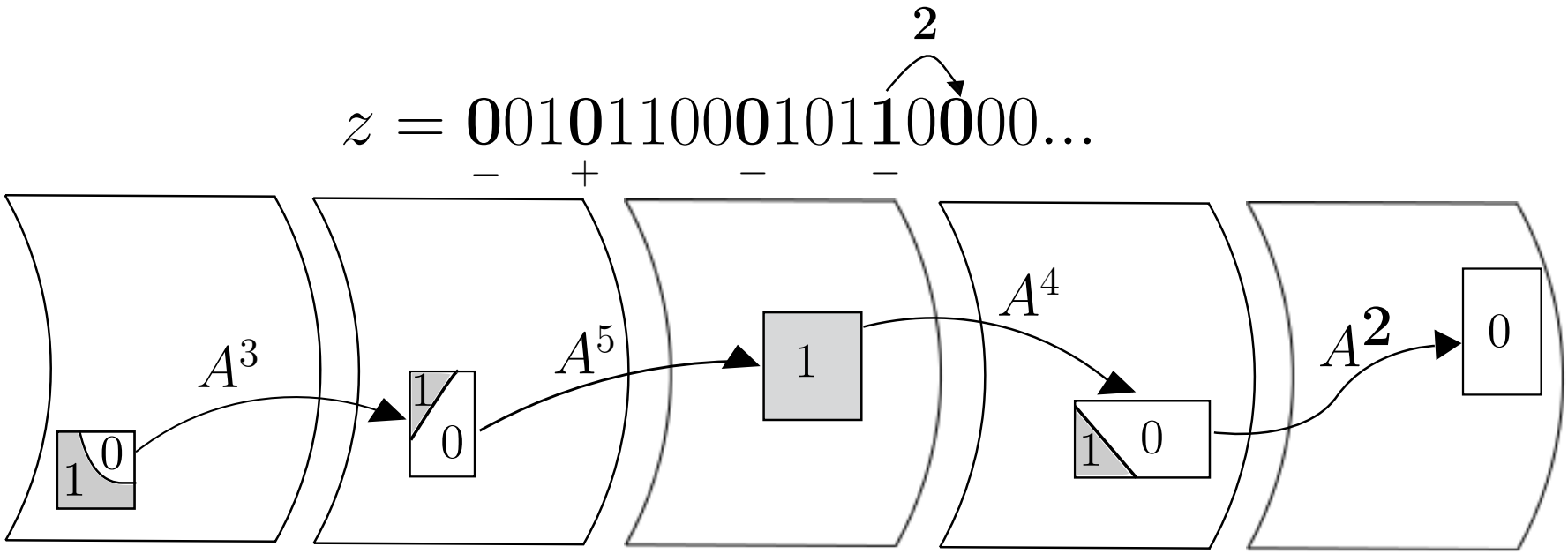



4
z = 0010110001011 10000...
− + −
A^3
A^5
A^4
A^2
1
0
1
0
1
0
1
0
1
0

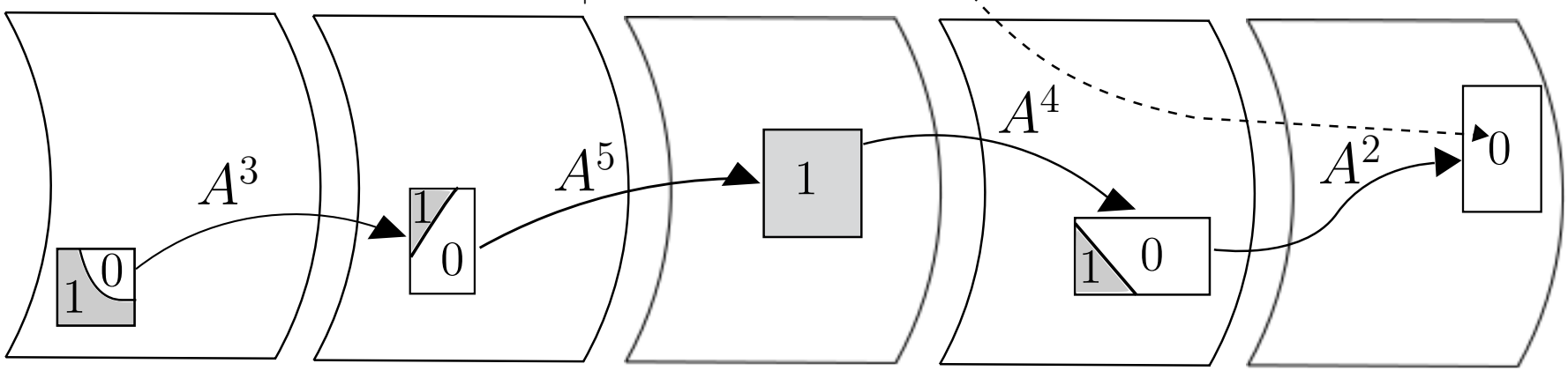

$z = \mathbf{0}01\mathbf{0}1100\mathbf{0}101\mathbf{1}0000...$
− + −
A^3
A^5
A^4
A^2
1
0
1
0
1
1
0
1
0
0

$$z = \mathbf{0}01\mathbf{0}1100\mathbf{0}101\mathbf{1}0000\ldots$$
$$\quad\; - \quad + \quad\;\; - \quad\;\; -$$

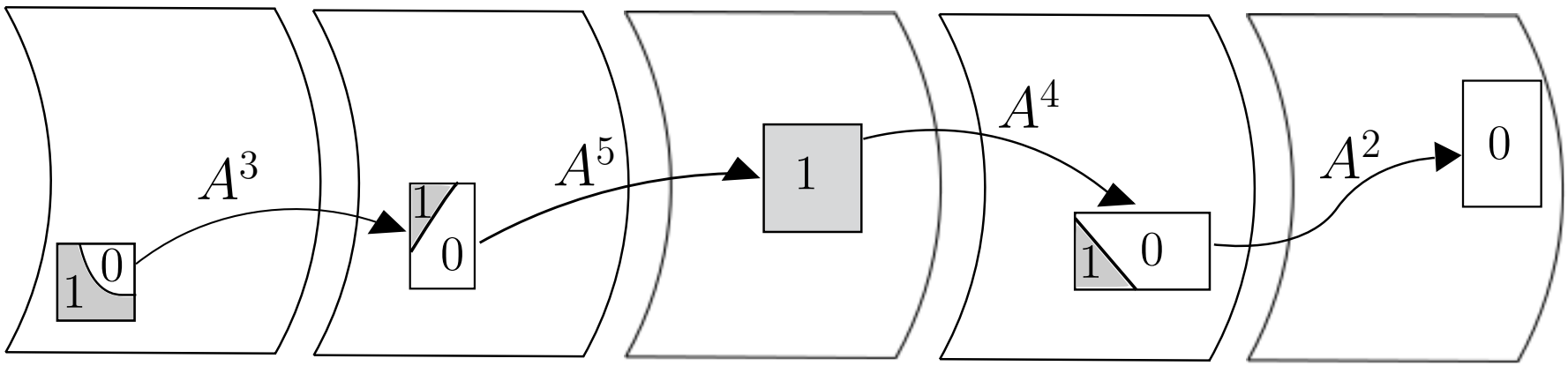



2
$z = 0010110001011000...$
− + − −
A^3
A^5
A^4
A^2
1
0
1
0
1
1
0
1
0
0

$$z = \mathbf{0}01\mathbf{0}1100\mathbf{0}101\mathbf{1}0\mathbf{0}00\ldots$$
$$\quad\; - \quad + \quad\;\; - \quad\;\; -$$

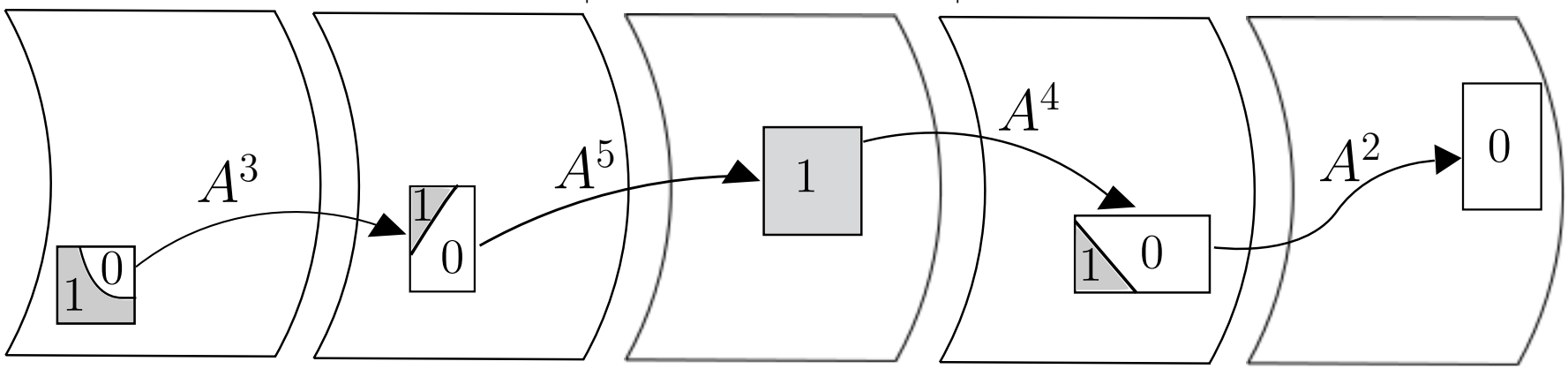


$$z = \mathbf{0}01\mathbf{0}1100\mathbf{0}101\mathbf{1}0\mathbf{0}00\ldots$$
$$\quad\; - \quad + \qquad - \qquad - \quad +$$



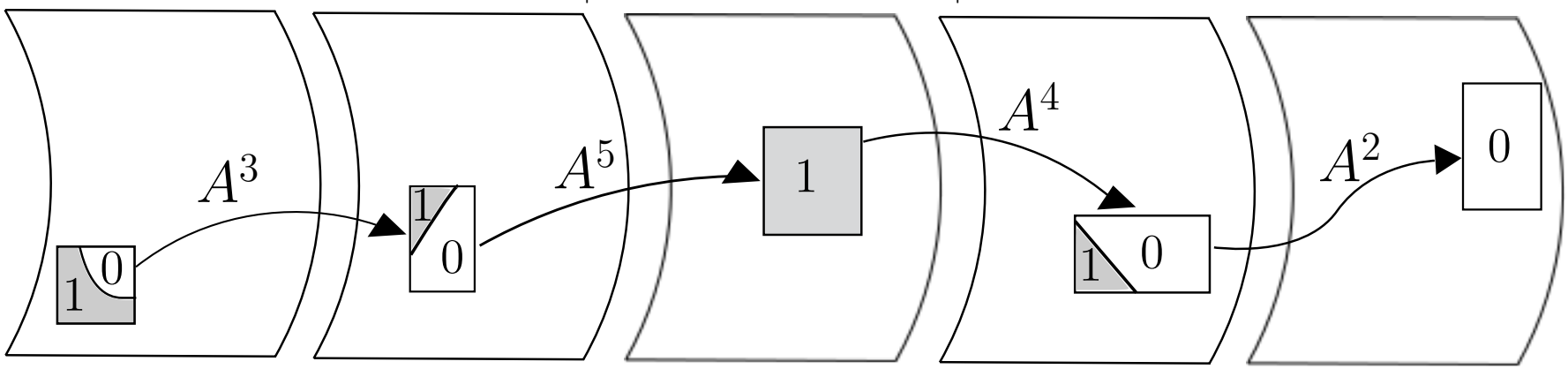
$$z = \mathbf{0}01\mathbf{0}1100\mathbf{0}101\mathbf{1}0\mathbf{0}00\ldots \text{ - rejected}$$

$$\begin{matrix} & - & + & & - & - & + \end{matrix}$$



$$z = \mathbf{0}01\mathbf{0}1100\mathbf{0}101\mathbf{1}0\mathbf{0}00\ldots \text{ - reject}$$

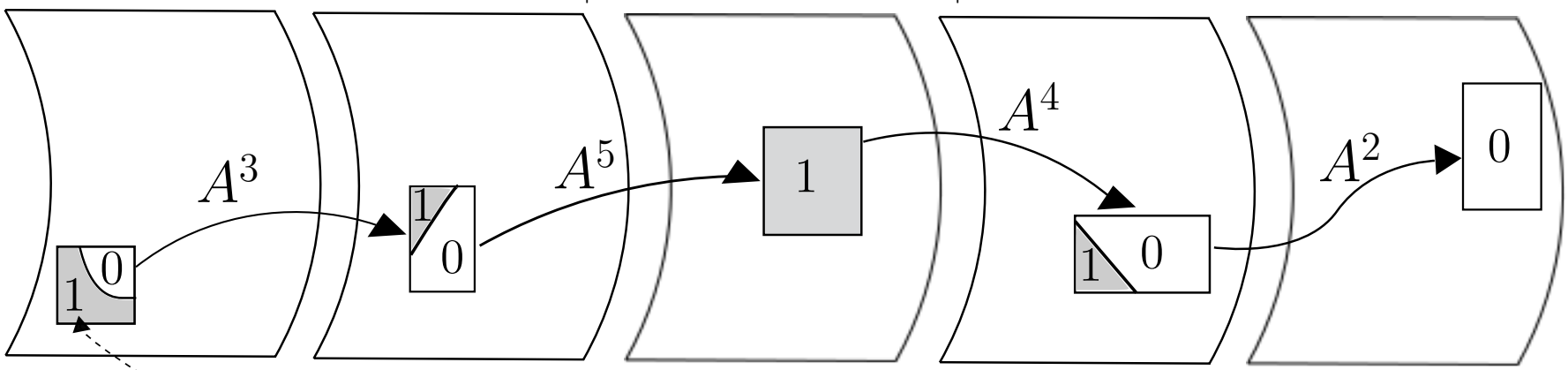
$$\begin{matrix} & - & + & & - & - & + \end{matrix}$$



$$z = 10101100010100000\ldots$$

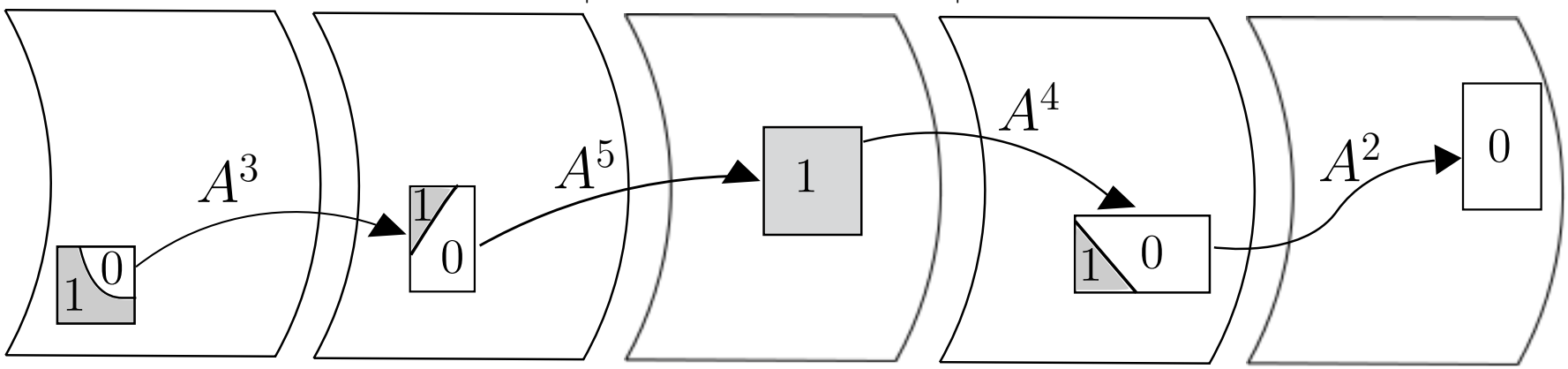
$$z = \mathbf{0}01\mathbf{0}1100\mathbf{0}101\mathbf{1}0\mathbf{0}00\ldots \text{ - reject}$$

$$- \quad + \qquad - \quad - \quad +$$



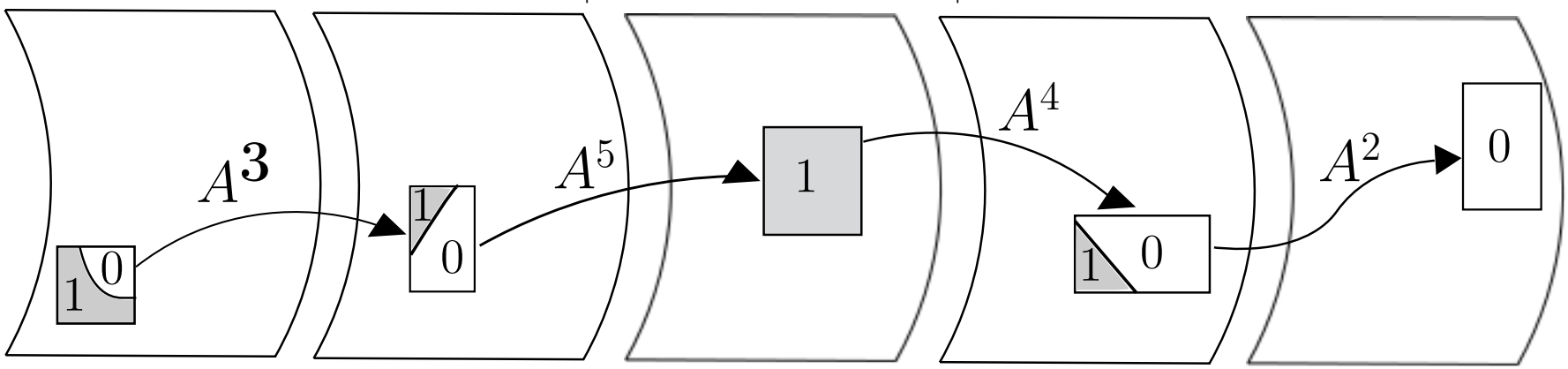
$$z = \mathbf{1}0101100010100000\ldots$$

$$z = \underset{-}{0}0\underset{+}{1}0\underset{-}{1}1\underset{-}{0}0\underset{+}{1}0\underset{-}{1}\underset{-}{1}\underset{+}{0}000\ldots \text{ - reject}$$



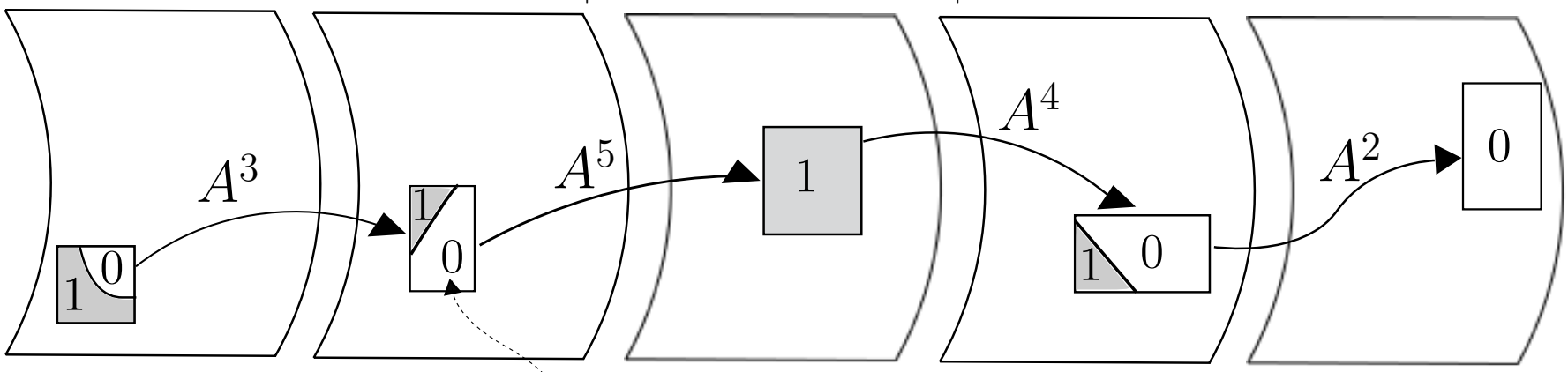
$$z = \underset{+}{1}0101100010100000\ldots$$

$$z = \mathbf{0}01\mathbf{0}1100\mathbf{0}101\mathbf{1}0\mathbf{0}00\ldots \text{ - reject}$$
$$ -+--+$$



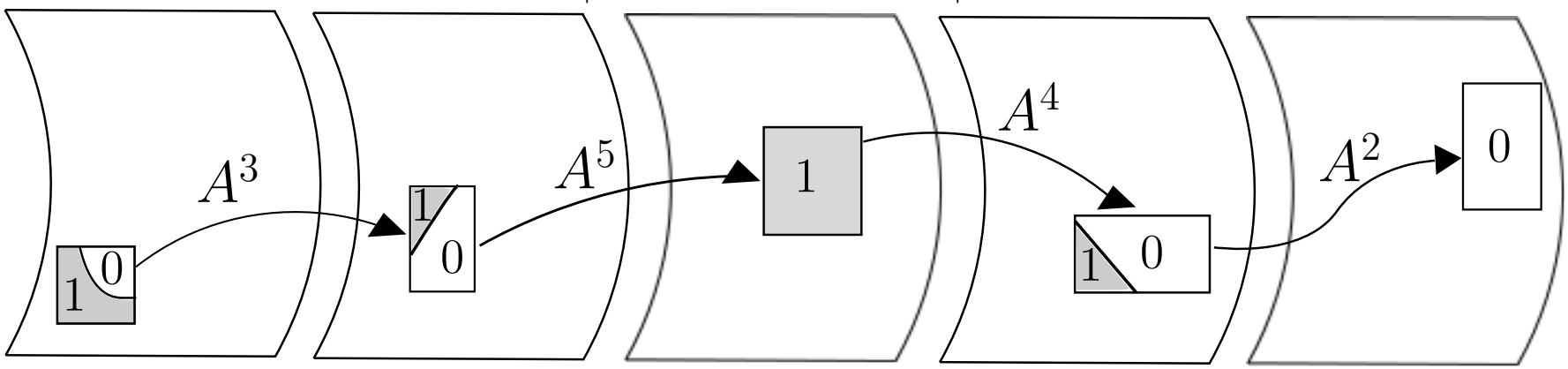
$$\mathbf{3}$$
$$z = \mathbf{1}01\mathbf{0}1100010100000\ldots$$
$$ +$$

$$z = \underset{-}{0}0\underset{+}{1}011\underset{-}{0}0\underset{-}{1}01\underset{-}{1}\underset{+}{0}000\ldots \text{ - reject}$$



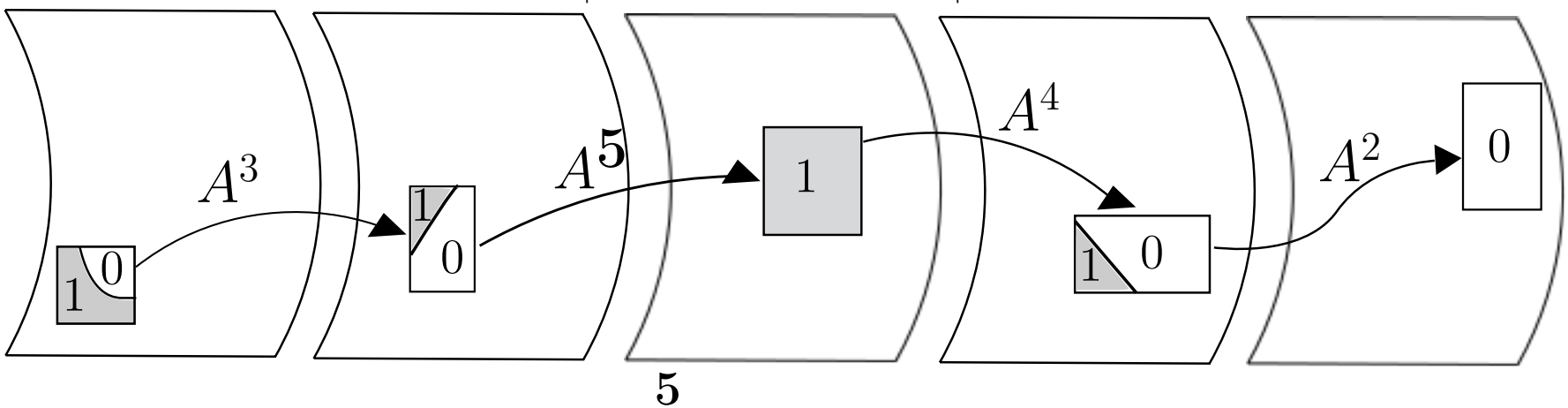
$$z = \underset{+}{1}01\underset{}{0}1100010100000\ldots$$

$$z = \underset{-}{\mathbf{0}}0\underset{+}{\mathbf{1}}1010\underset{-}{\mathbf{0}}1011\underset{-}{\mathbf{0}}\underset{+}{\mathbf{1}}0000\ldots \text{ - reject}$$



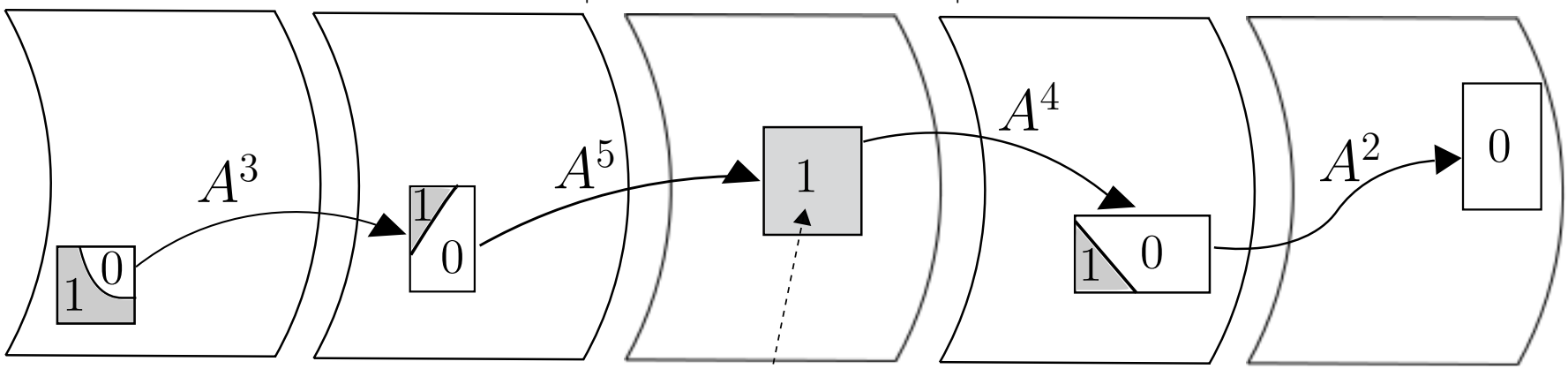
$$z = \underset{+}{\mathbf{1}}01\underset{+}{\mathbf{0}}1100010100000\ldots$$

$$z = \mathbf{0}01\mathbf{0}1100\mathbf{0}101\mathbf{1}0\mathbf{0}00\ldots \text{ - reject}$$
$$ - \quad + \quad- \quad - \quad +$$



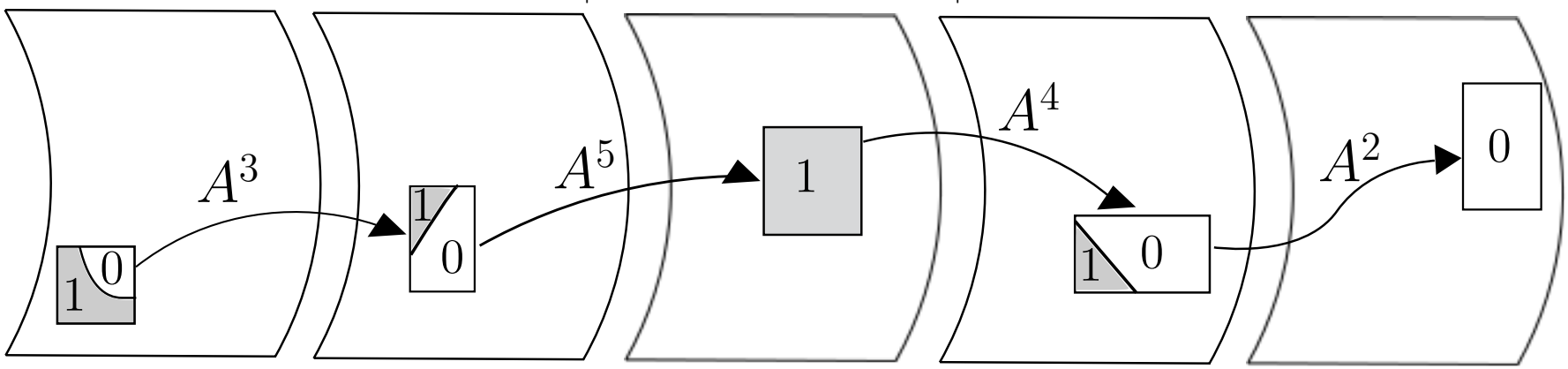
$$\overset{\mathbf{5}}{\frown}$$
$$z = \mathbf{1}01\mathbf{0}1100\mathbf{0}10100000\ldots$$
$$ + \quad + \quad$$

$$z = \underset{-}{\mathbf{0}}0\underset{+}{\mathbf{1}}1\underset{-}{\mathbf{0}}0\underset{-}{\mathbf{1}}0\underset{-}{\mathbf{1}}\underset{+}{\mathbf{0}}0\ldots \text{ - reject}$$



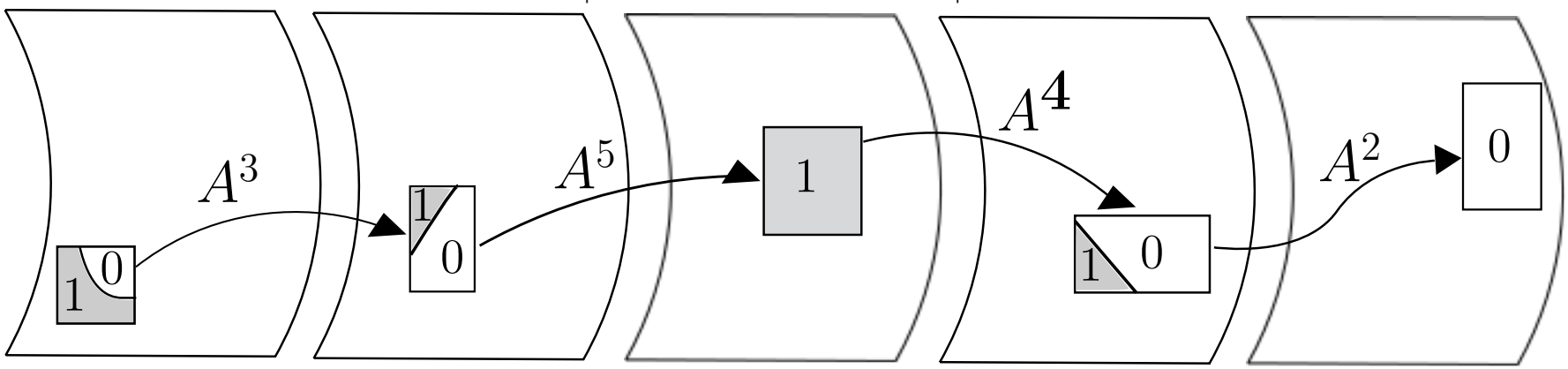
$$z = \underset{+}{\mathbf{1}}0\underset{+}{\mathbf{1}}1\mathbf{0}0\mathbf{0}10100000\ldots$$

$$z = \underset{-}{\mathbf{0}}0\underset{+}{\mathbf{1}}1100\underset{-}{\mathbf{1}}01\underset{-}{\mathbf{1}}0\underset{+}{\mathbf{0}}000\ldots \text{ - reject}$$



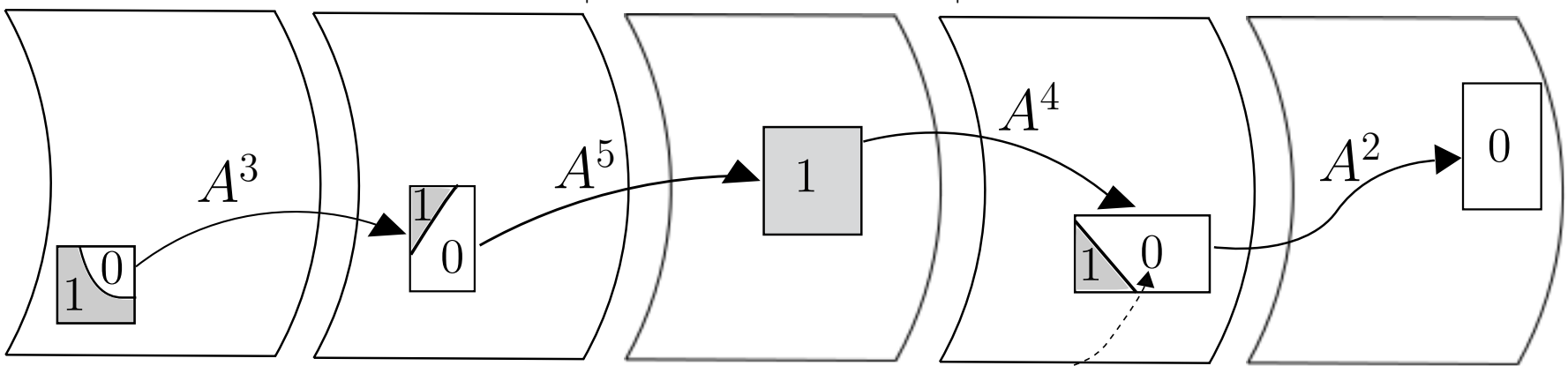
$$z = \underset{+}{\mathbf{1}}0\underset{+}{\mathbf{1}}1100\underset{-}{\mathbf{0}}10100000\ldots$$

$$z = \mathbf{0}01\mathbf{0}1100\mathbf{0}101\mathbf{1}0\mathbf{0}00\ldots \text{ - reject}$$
$$ -+--+$$



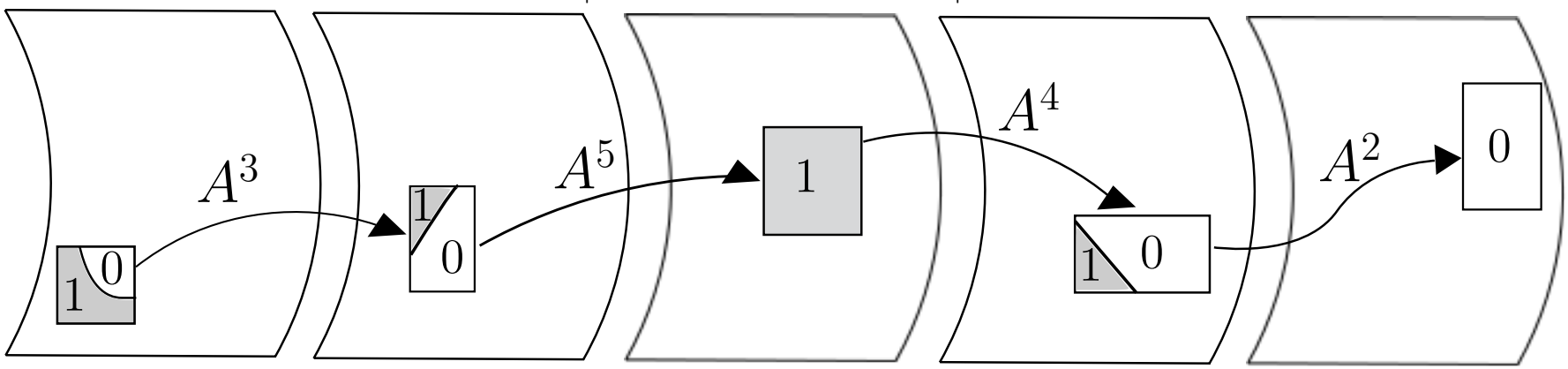
$$\mathbf{4}$$
$$z = \mathbf{1}01\mathbf{0}1100\mathbf{0}101\mathbf{0}0000\ldots$$
$$ ++-$$

$$z = \underset{-}{\mathbf{0}}01\underset{+}{\mathbf{0}}1100\underset{-}{\mathbf{0}}101\underset{-}{\mathbf{1}}0\underset{+}{\mathbf{0}}000\ldots \text{ - reject}$$



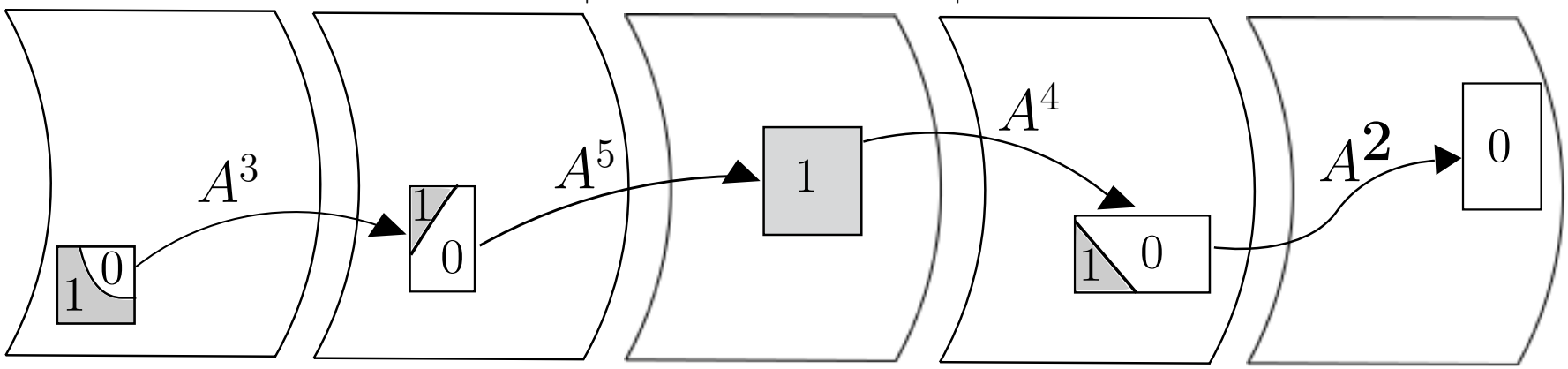
$$z = \underset{+}{\mathbf{1}}01\underset{+}{\mathbf{0}}1100\underset{-}{\mathbf{0}}101\underset{}{\mathbf{0}}00000\ldots$$

$$z = \underset{-}{\mathbf{0}}0\underset{+}{\mathbf{0}}11\underset{-}{0}0\underset{-}{\mathbf{1}}0\underset{+}{\mathbf{1}}\mathbf{0}000\ldots \text{ - reject}$$



$$z = \underset{+}{\mathbf{1}}0\underset{+}{\mathbf{1}}11\underset{-}{0}0\underset{+}{\mathbf{1}}0\mathbf{0}000\ldots$$

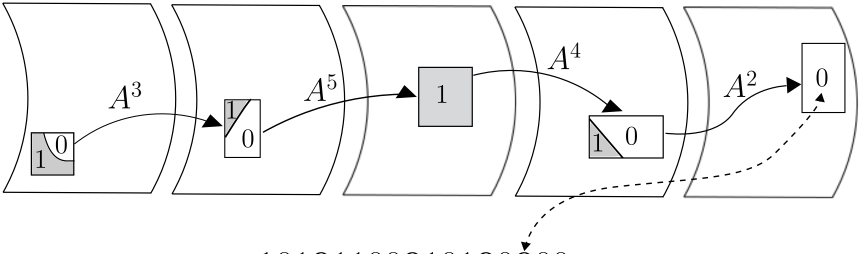
$$z = \mathbf{0}01\mathbf{0}1100\mathbf{0}101\mathbf{1}0\mathbf{0}00\ldots \text{ - reject}$$
$$ - \quad + \quad- \quad - \quad +$$



$$\mathbf{2}$$
$$z = \mathbf{1}01\mathbf{0}1100\mathbf{0}101\mathbf{0}0\mathbf{0}00\ldots$$
$$ +\quad +\quad-\quad +$$

$$z = \mathbf{0}01\mathbf{0}1100\mathbf{0}101\mathbf{1}0\mathbf{0}00\ldots \text{ - reject}$$

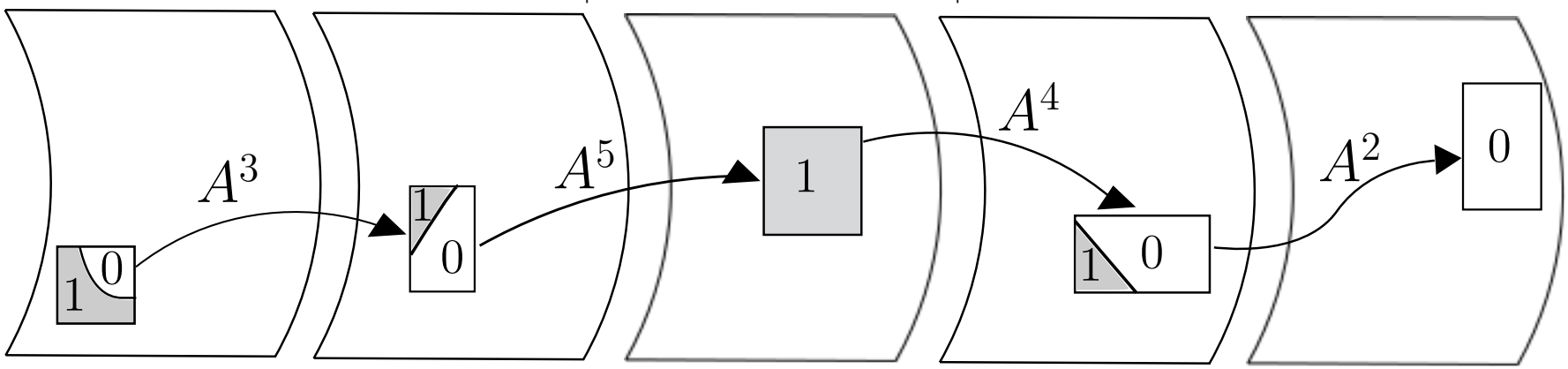
$-\quad +\quad -\quad -\quad +$



$$z = \mathbf{1}01\mathbf{0}1100\mathbf{0}101\mathbf{0}0\mathbf{0}00\ldots$$

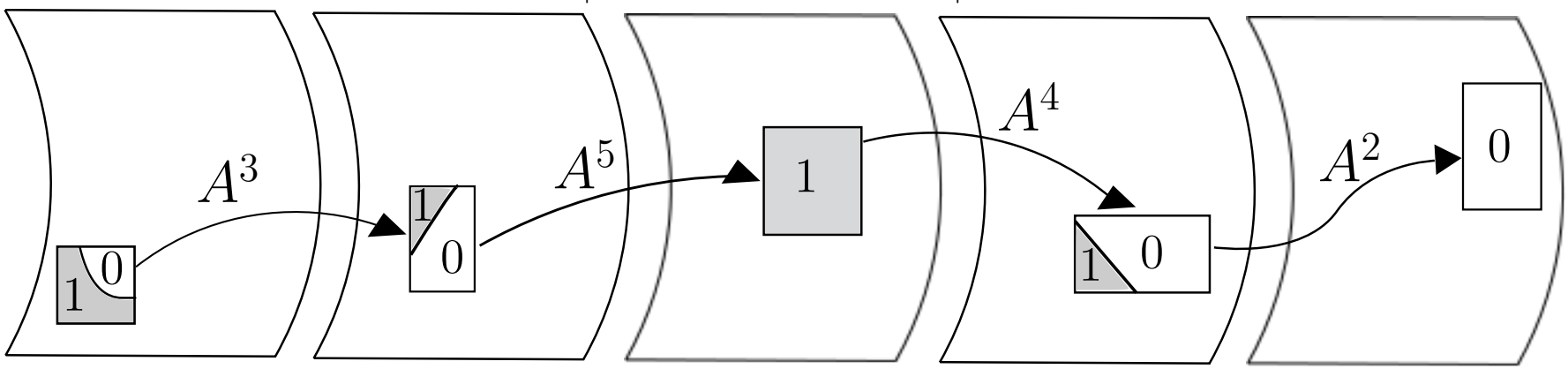
$+\quad +\quad -\quad +$

$$z = \underset{-}{\mathbf{0}}0\underset{+}{\mathbf{1}}1\underset{-}{\mathbf{0}}0\underset{-}{\mathbf{1}}0\underset{+}{\mathbf{1}}\underset{-}{\mathbf{0}}\underset{+}{\mathbf{0}}000\ldots \text{ - reject}$$



$$z = \underset{+}{\mathbf{1}}0\underset{+}{\mathbf{1}}1\underset{-}{\mathbf{0}}0\underset{+}{\mathbf{1}}\underset{+}{\mathbf{0}}\underset{-}{\mathbf{0}}000\ldots$$

$$z = \underset{-}{\mathbf{0}}01\underset{+}{\mathbf{0}}1100\underset{-}{\mathbf{0}}101\underset{-}{\mathbf{1}}0\underset{+}{\mathbf{0}}000\ldots \text{ - rejected}$$

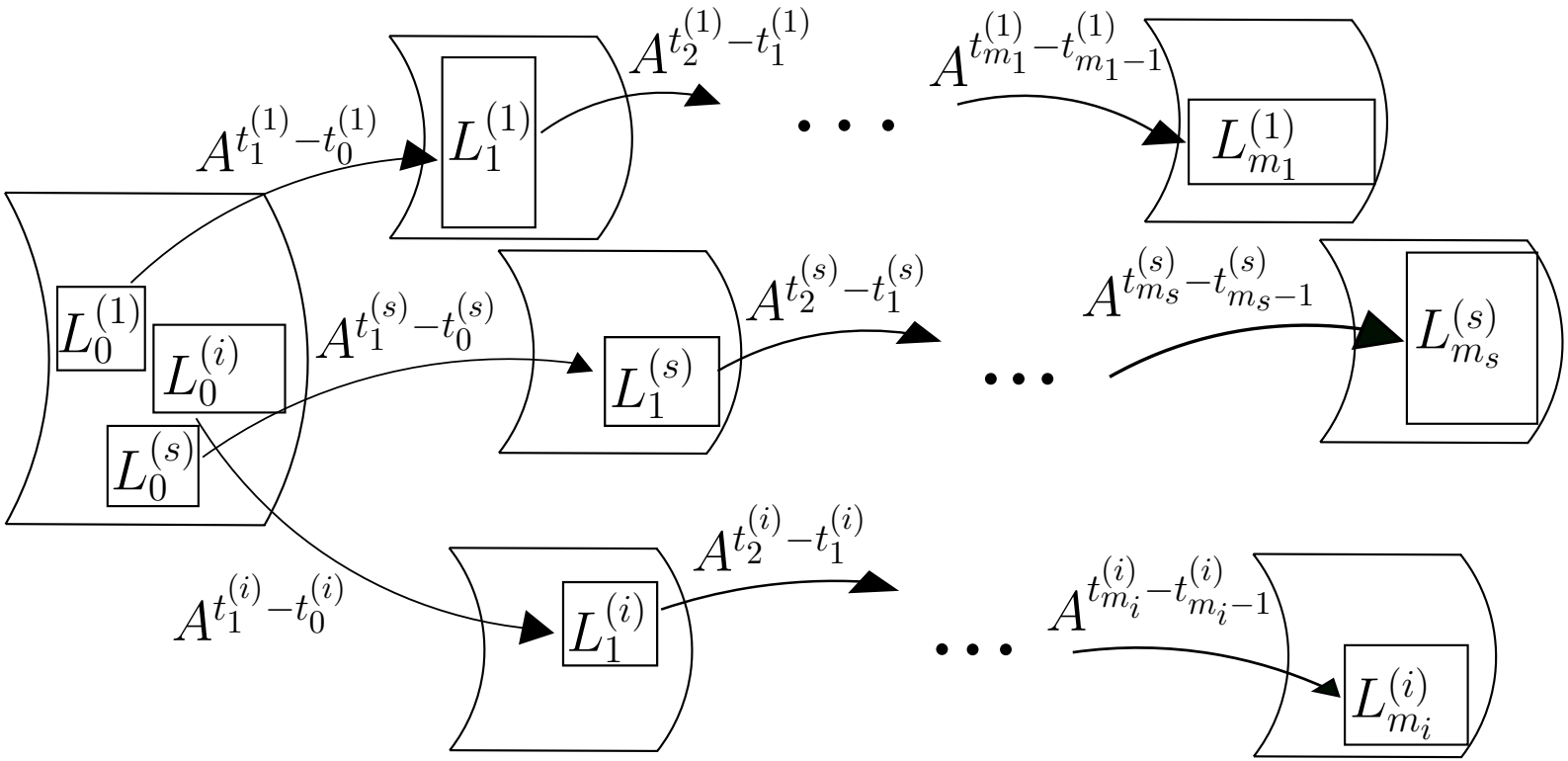


$$z = \underset{+}{\mathbf{1}}01\underset{+}{\mathbf{0}}1100\underset{-}{\mathbf{0}}101\underset{+}{\mathbf{0}}0\underset{+}{\mathbf{0}}000\ldots \text{ - accepted}$$

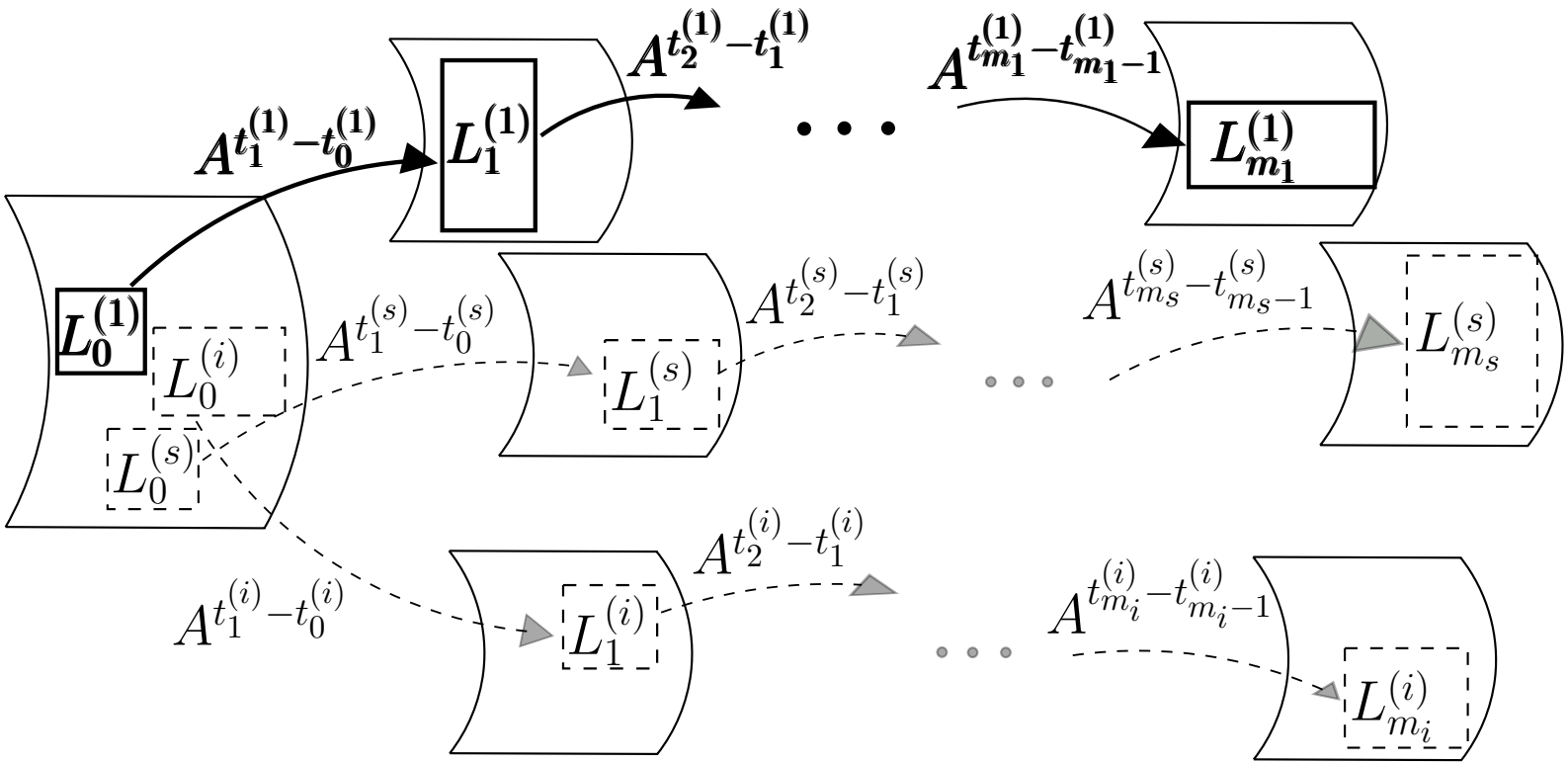
The efficiency of the method depends on:

- how close the function f on such planes is to a constant, i.e. $\mathrm{wt}(f)$ on planes;
- number of unbalanced planes.

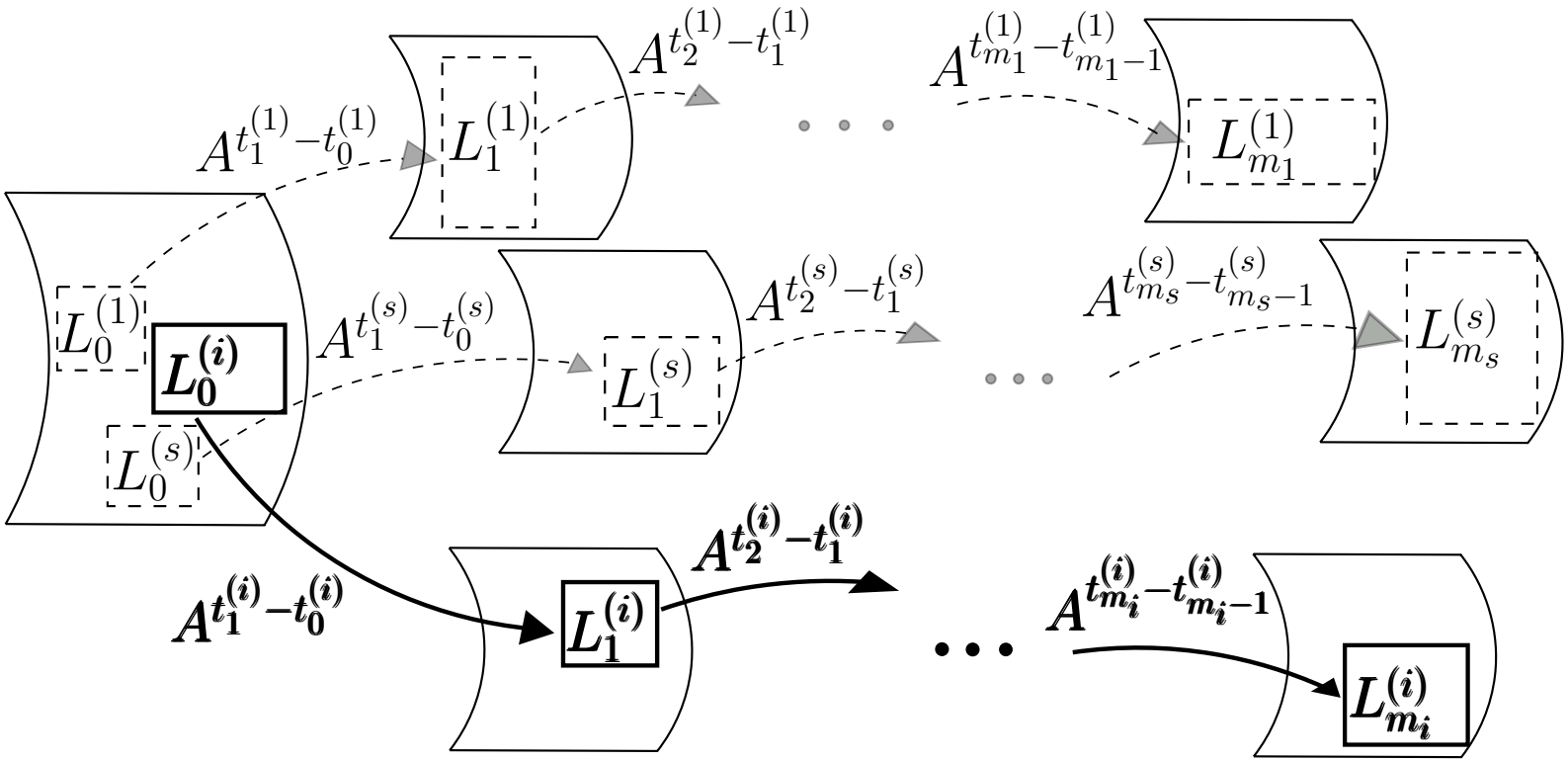
$$z_i = f(A^i u^*), \quad i = \overline{0, N-1}.$$



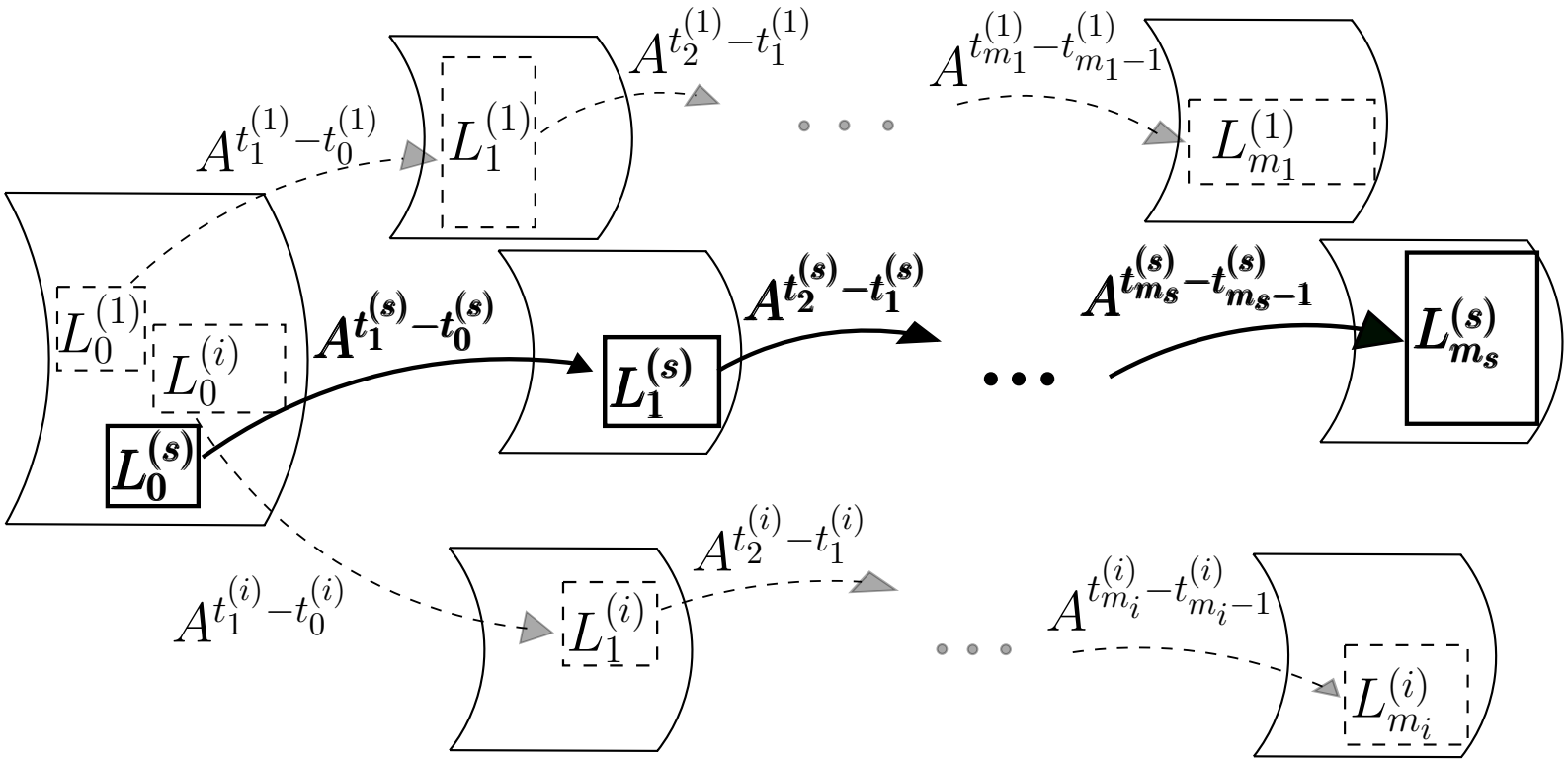
$$z_i = f(A^i u^*), \quad i = \overline{0, N-1}.$$



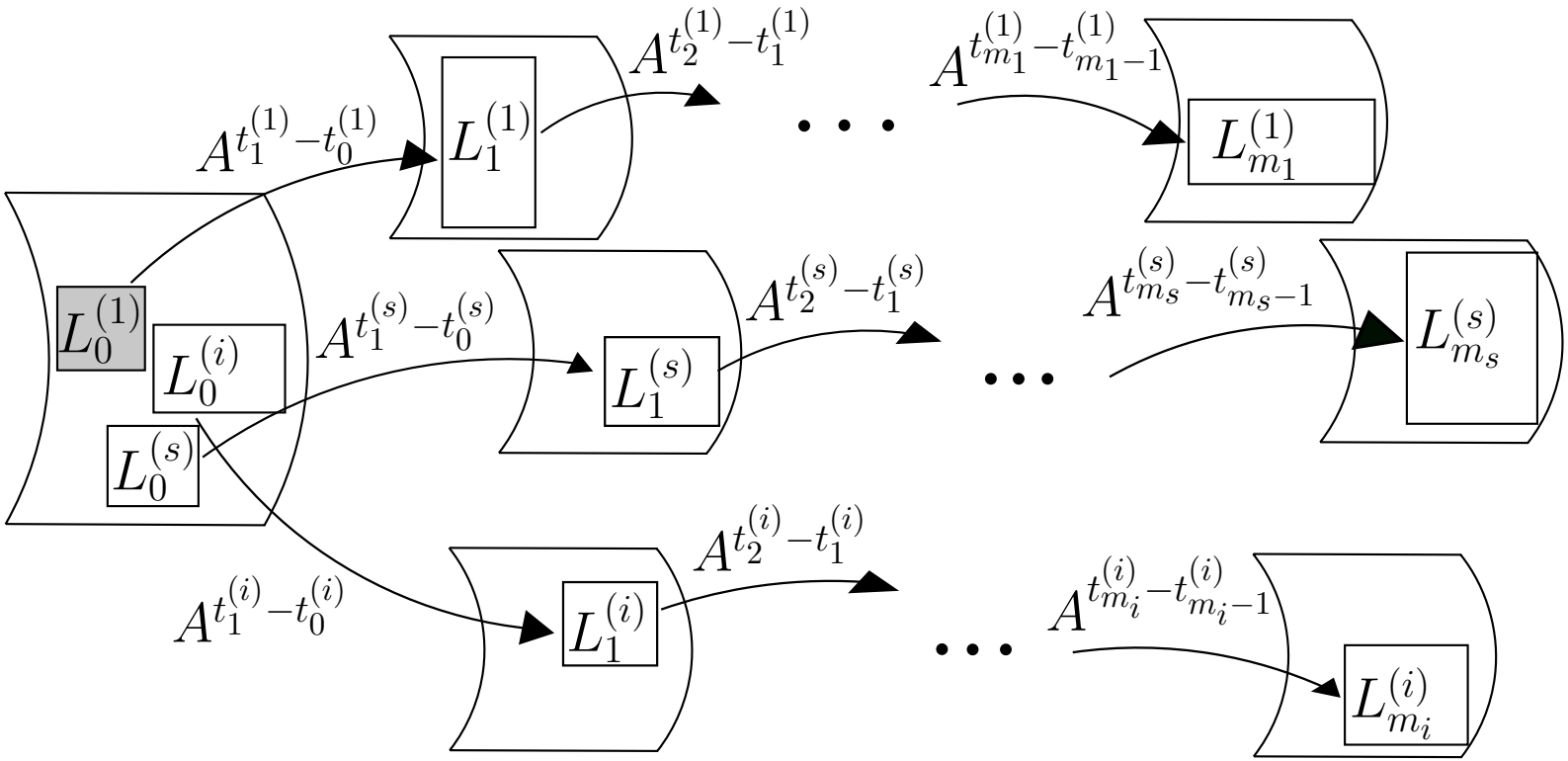
$$z_i = f(A^i u^*), \quad i = \overline{0, N-1}.$$



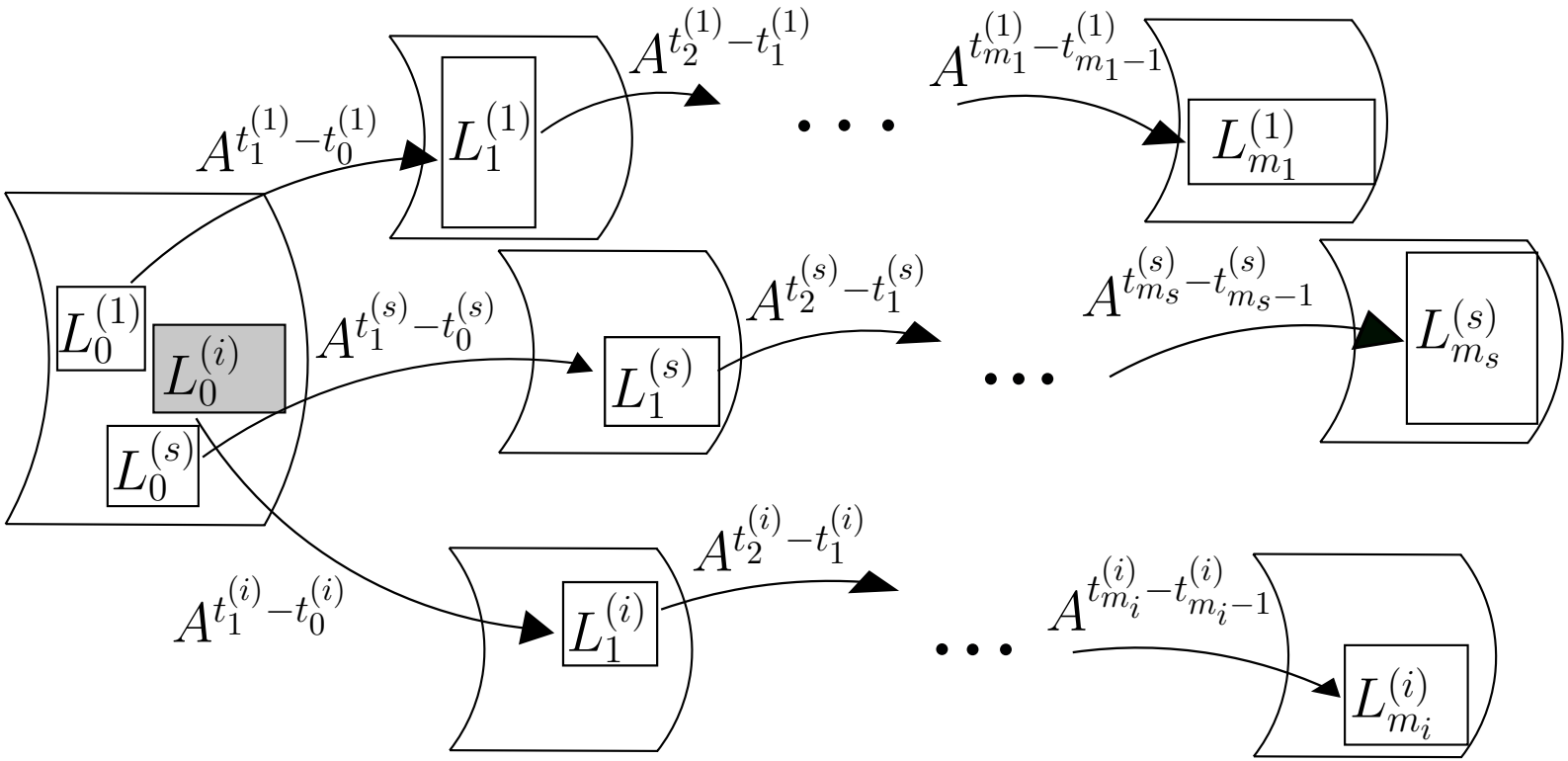
$$z_i = f(A^i u^*), \quad i = \overline{0, N-1}.$$



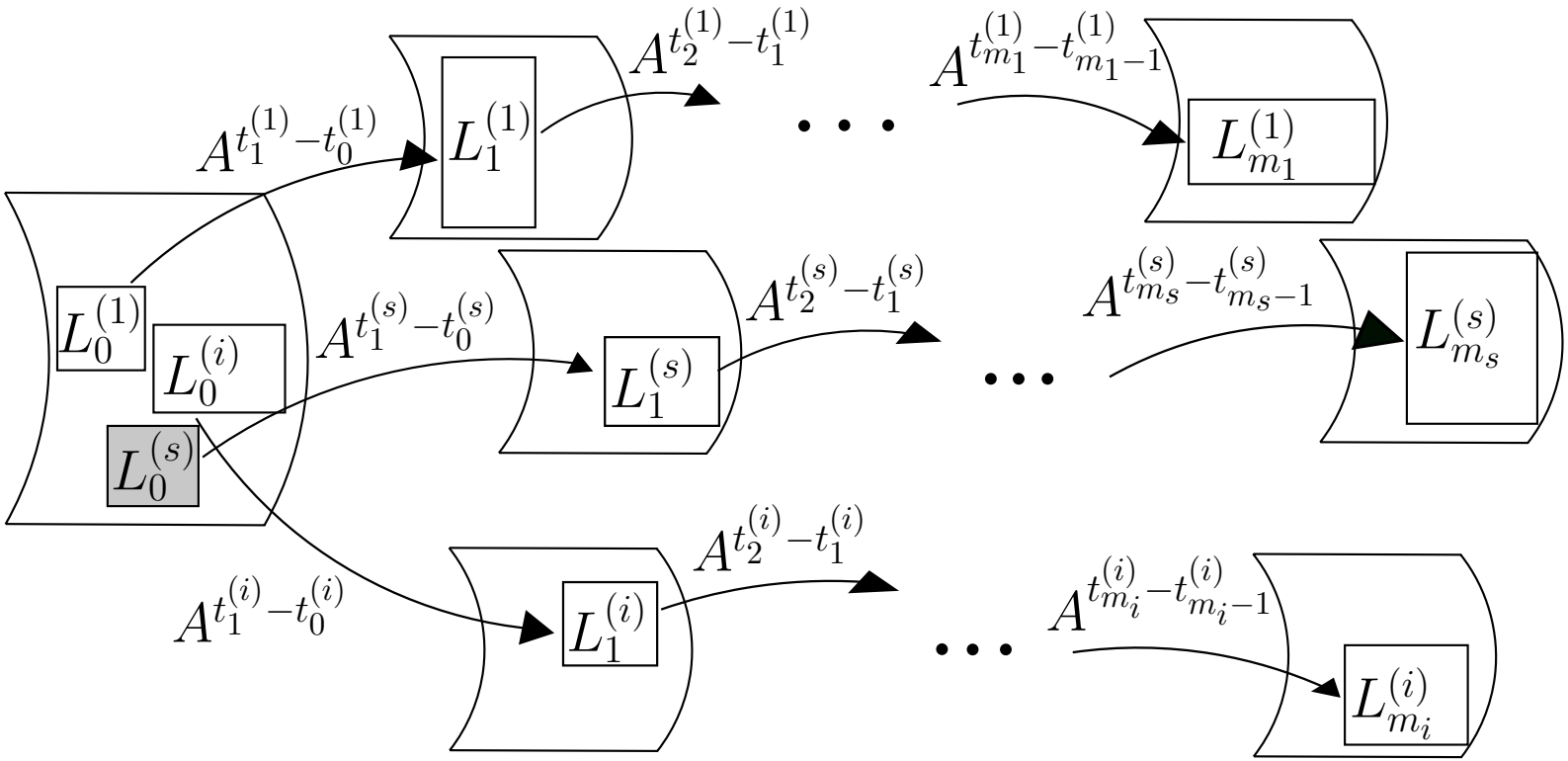
$$z_i = f(A^i u^*), \quad i = \overline{0, N-1}.$$



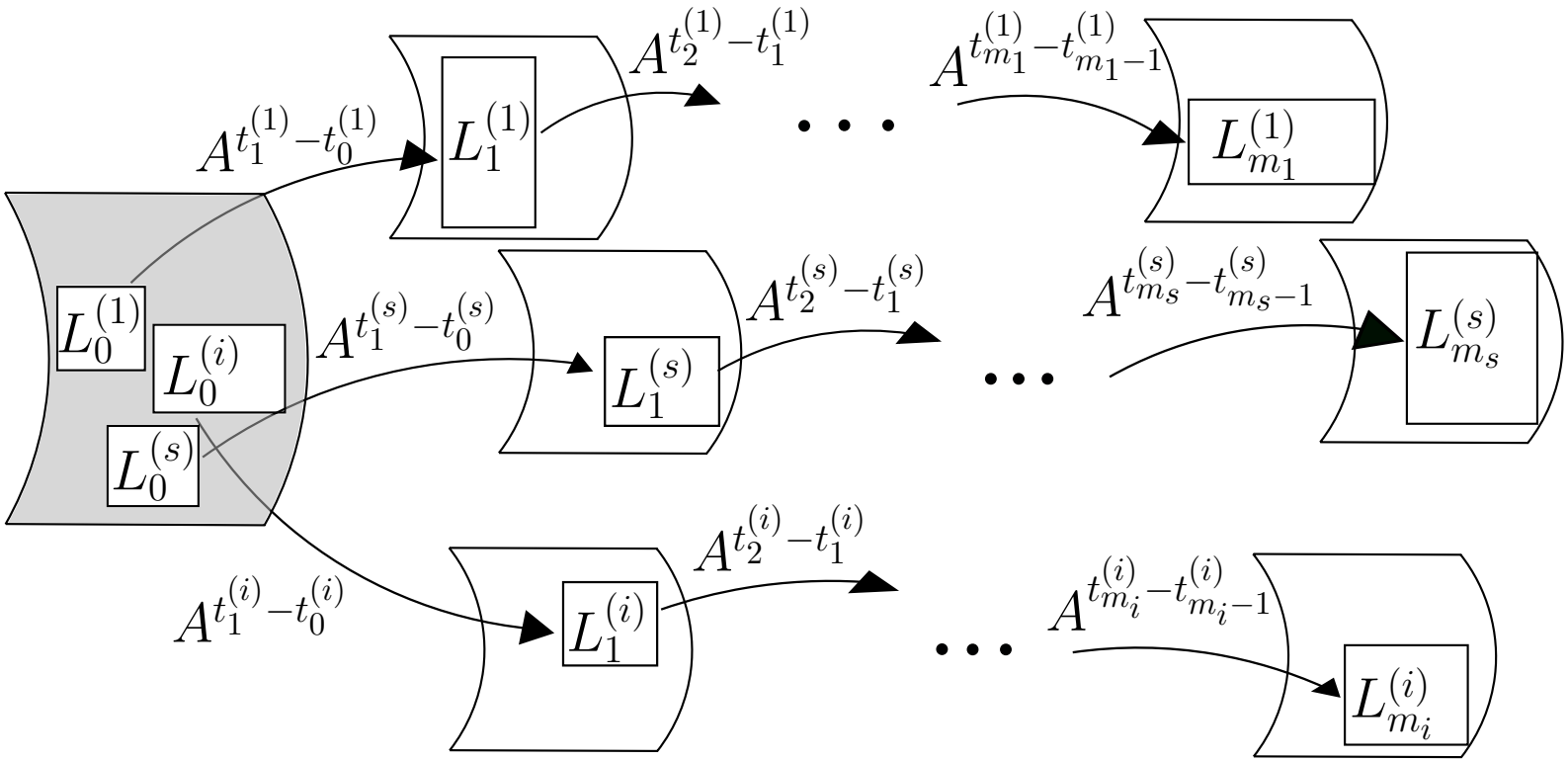
$$z_i = f(A^i u^*), \quad i = \overline{0, N-1}.$$



$$z_i = f(A^i u^*), \quad i = \overline{0, N-1}.$$



$$z_i = f(A^i u^*), \quad i = \overline{0, N-1}.$$



Method description

- Selecting the «correct» trajectories.
- Thorough testing of the «correct» trajectories.
- Viewing the set of uncovered vectors.

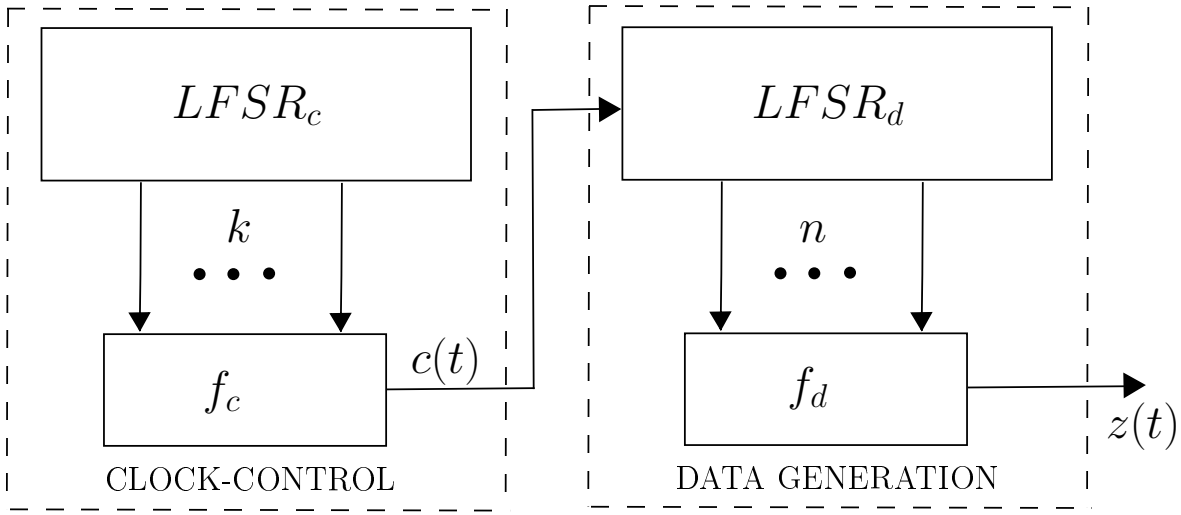


Figure 1: LILI-128

- DATA GENERATION: $2^{89} \rightarrow 2^{76}$
- CLOCK-CONTROL: $2^{39} \rightarrow 2^{23}$
- LILI-128: $2^{128} \rightarrow 2^{118}$

- A full description of the method, evaluation of characteristics and examples can be found in *Alekseev E.K., Kuschinskaya L.A.* «Generalization of one method of a filter generator key recovery», Discrete Mathematics and Applications, Volume 29 (2019), Issue 2, Pages 69–87.

Resistance condition

Is it possible to ensure generator resistance againts the method by selecting the Boolean function?

Resistance condition

Is it possible to ensure generator resistance againts the method by selecting the Boolean function?

- Siegenthaler's method $\rightarrow$ high order correlation immunity.
- Previously described method $\rightarrow$?

Further we will say that a certain plane of the space V_n is f-balanced (f-unbalanced)) if the function f is balanced (unbalanced) on this plane.

Statement

For any function $f \in \mathcal{F}_n$ and for any k, $1 \leqslant k \leqslant n-1$, there exists a plane of space V_n of dimension k that is f-unbalanced.

Definition

The plane weight characteristic $\mathrm{pwc}_d(f)$ of a function f of order d, $1 \leqslant d \leqslant n$, is a vector of length $2^{d-1}+1$, the w-th component of which is equal to the number of planes of dimension d on which the weight of function f is equal to either $2^{d-1}-w$ or $2^{d-1}+w$ $(0 \leqslant w \leqslant 2^{d-1})$.

For example, for functions of 5 variables identically equal to 0 and 1, planar weight characteristics of order 3 are the same and equal $(0,0,0,0,620)$.

For natural $n \geqslant 2$ and k, $1 \leqslant k \leqslant n-1$, let $\mathcal{P}_{n,k}$ be the number of planes of dimension k of the space V_n. That is

$$\mathcal{P}_{n,k} = 2^{n-k} \cdot \prod_{i=1}^{k} \frac{2^n - 2^{i-1}}{2^k - 2^{i-1}}.$$

Statement

Any non-constant affine function $f \in \mathcal{F}_n$ on any plane is either balanced or constant. Also for any k, $2 \leqslant k \leqslant n-2$, the following ratio is true

$$pwc_k(f) = (\mathcal{P}_{n,k} - 2 \cdot \mathcal{P}_{n-1,k}, 0, 0, \ldots, 0, 2 \cdot \mathcal{P}_{n-1,k}).$$

The number of unbalanced planes

For the Boolean function $f \in \mathcal{F}_n$ let $S_f(k)$ be the number of planes of dimension $1 \leqslant k \leqslant n$ on which the weight of the function is different from 2^{k-1}, that is, on which the function is unbalanced.

Statement

For a Boolean function $f \in \mathcal{F}_n$ of the weight w, the number of unbalanced planes of dimension 1 is equal to

$$S_f(1) = \frac{w(w-1)}{2} + \frac{(2^n - w)(2^n - w - 1)}{2}.$$

Theorem

Let $f \in \mathcal{F}_n$. The following statements hold:

1. *For a balanced Boolean function $f \in \mathcal{F}_n$, the number of unbalanced hyperplanes is equal to twice a number of non-zero Walsh-Hadamard coefficients. In other words,*

$$S_f(n-1) = 2 \cdot |\{u \in V_n | W_f(u) \neq 0\}|.$$

2. *If for some k, $2 \leqslant k \leqslant n-1$, then the number of unbalanced planes of dimension $k-1$ satisfies the inequality*

$$S_f(k-1) \geqslant t \cdot (2^k - 1) - \frac{t \cdot (t+1)}{2},$$

where $t = \min(2^k - 1, S_f(k) - 1)$.

- $f \in \mathcal{F}_5$, $f = 00017\mathrm{FFF}$, $wt(f) = 16$.

- $f \in \mathcal{F}_5$, $f = 00017FFF$, $wt(f) = 16$.

Dimension	Real value	Based on theorem
4	32	32
3	270	105
2	490	21
1	240	3

Function weight on planes

Theorem

Let natural n and k be such that $n \geqslant 2$ and $1 \leqslant k \leqslant n-1$. Then for any Boolean function f of n variables, any subspace L of the space V_n of dimension k and any vector $a \in V_n$, the following inequality is valid

$$\left| \mathrm{wt}\left(f|_{a \oplus L}\right) - \frac{\mathrm{wt}\left(f\right)}{2^{n-k}} \right| \leqslant \left(1 - \frac{1}{2^{n-k}}\right) \cdot \left(2^{n-1} - \mathrm{nl}\left(f\right)\right).$$

Function weight on planes

- $n = 10$, $f_d \in \mathcal{F}_n$ — filter function from LILI-128. $\mathrm{wt}\,(f_d) = 512$, $\mathrm{nl}\,(f_d) = 480$.

dim	$\mathrm{wt}\,(f_d\|_{L\oplus a})_{th}$	$\mathrm{wt}\,(f_d\|_{L\oplus a})_{ex}$	tests count
9	256 ± 16	256 ± 16	2^{10}
8	128 ± 24	128 ± 24	2^{18}
7	64 ± 28	64 ± 20	2^{18}
6	32 ± 30	32 ± 20	2^{22}
5	16 ± 16	16 ± 16	2^{22}

- Let $\mathfrak{GU}(V_n)\mathfrak{H}_d$ be a set of triples (A, b, h), where A is a nondegenerate $n \times n$-matrix over the field $\mathbb{F}_2$, $b \in V_n$, and h is a function from $\mathcal{F}_n$ such that $\deg(h) \leqslant d$.
- $\alpha = (A, b, h) \in \mathfrak{GU}(V_n)\mathfrak{H}_d$, $f^\alpha(x) = f(Ax \oplus b) \oplus h(x)$

Statement

For any function $f \in \mathcal{F}_n$, any natural $d, 1 \leqslant d \leqslant n$, , and any element $\alpha \in \mathfrak{GU}(V_n)\mathfrak{H}_0$ the planar weight characteristic $\mathrm{pwc}_d(f)$ and $\mathrm{pwc}_d(f^\alpha)$ coincide.

Functions of the weight 16

№	$\lvert\{f\}_{\mathfrak{GU}(V_5)\mathfrak{H}_0}\rvert$	$\deg(f)$	$\mathrm{nl}(f)$	4	3	2	1
1	62	1	0	**2**	**60**	**280**	240
2	15872	4	2	32	270	**490**	240
3	59520	3	4	16	326	616	240
4	833280	4	4	40	362	622	240
5	555520	4	6	32	342	682	240
6	9999360	4	6	40	394	694	240
7	8888320	4	6	44	410	700	240
8	8680	2	8	**8**	**204**	664	240
9	1666560	4	8	36	366	706	240
10	312480	3	8	20	402	712	240
11	1249920	4	8	44	418	718	240
12	9999360	4	8	42	425	730	240
13	555520	3	8	26	**446**	736	240
14	1666560	4	8	50	432	742	240
15	833280	3	8	20	362	712	240
16	4999680	4	8	44	398	718	240
17	53329920	4	8	42	410	730	240
18	39997440	4	8	46	426	736	240
19	9999360	4	8	42	425	730	240

Functions of the weight 16

№	$\lvert\{f\}_{\mathfrak{GU}(V_5)\mathfrak{H}_0}\rvert$	$\deg(f)$	$\mathrm{nl}(f)$	4	3	2	1
20	39997440	4	8	46	426	736	240
21	9999360	3	8	26	426	736	240
22	19998720	4	8	50	422	742	240
23	1666560	4	8	50	432	742	240
24	13332480	4	10	40	422	742	240
25	9999360	4	10	40	432	742	240
26	79994880	4	10	44	438	748	240
27	39997440	4	10	48	429	754	240
28	444416	4	10	32	360	730	240
29	19998720	4	10	40	412	742	240
30	6666240	4	10	48	384	754	240
31	53329920	4	10	44	428	748	240
32	79994880	4	10	48	424	754	240
33	39997440	4	10	48	429	754	240
34	31997952	4	10	52	440	760	240
35	1666560	3	12	32	400	760	240
36	1666560	4	12	**56**	436	**766**	240
37	5332992	3	12	32	440	760	240
38	27776	2	12	32	240	760	240

The classification of Bent functions of 6 variables under the group $\mathfrak{GU}(V_6)\mathfrak{H}_1$ was proposed in *Rothaus O.S.* «On bent functions», J. Comb. Theory. 1979. Ser. A., V. 20., P. 300–305.

№	$\deg(f)$	$\mathrm{nl}(f)$	5	4	3	2	1
1	2	28	63	1659	5175	6636	1008
2	3	28	63	1659	7415	6636	1008
3	3	28	63	1659	7975	6636	1008
4	3	28	63	1659	8255	6636	1008

- The classification of Boolean functions of 5 variables with respect to the group $\mathfrak{GU}(V_5)\mathfrak{H}_0$ can be found in *Alekseev E.K., Kuschinskaya L.A.* «Weights on affine subspaces and some other cryptographic characteristics of Boolean functions of 5 variables». Cryptology ePrint Archive: Report 2019/559.
- For each of these functions, the values of parameters are given, which coincide for all functions from the corresponding equivalence class. Namely, the power of the equivalence class, the algebraic degree, the nonlinearity and the number of unbalanced planes of dimensions $4, 3, 2, 1$.

Thank you for your attention!

alekseev@cryptopro.ru
lyudmila.kuschinskaja@yandex.ru