Matematyczna podróż

w głąb Enigmy

Warszawa, Kwiecień 2016

Barbara Roszkowska-Lech

WYDZIAŁ
MATEMATYKI I NAUK
INFORMACYJNYCH

Przyspieszony kurs teorii permutacji

Definicja

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$$

WYDZIAŁ MATEMATYKI I NAUK INFORMACYJNYCH

$$\begin{pmatrix} A & E & G & I & N & M \\ E & G & N & I & M & A \end{pmatrix}$$

WYDZIAŁ
MATEMATYKI I NAUK
INFORMACYJNYCH

$$\begin{pmatrix} A & E & G & I & N & M \\ E & G & N & I & M & A \end{pmatrix}$$

$$\begin{pmatrix} E & G & N & I & M & A \\ E & N & I & G & M & A \end{pmatrix}$$

WYDZIAŁ MATEMATYKI I NAUK INFORMACYJNYCH

$$\begin{pmatrix} A & E & G & I & N & M \\ E & G & N & I & M & A \end{pmatrix}$$

$$\begin{pmatrix} E & G & N & I & M & A \\ E & N & I & G & M & A \end{pmatrix}$$

$$\begin{pmatrix} E & G & N & I & M & A \\ E & N & I & G & M & A \end{pmatrix} \circ \begin{pmatrix} A & E & G & I & N & M \\ E & G & N & I & M & A \end{pmatrix} =$$

$$\begin{pmatrix} A & E & G & I & N & M \\ E & N & I & G & M & A \end{pmatrix}$$

WYDZIAŁ MATEMATYKI I NAUK INFORMACYJNYCH

Definicja

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$$

Definicja

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$$

$$\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

WYDZIAŁ MATEMATYKI I NAUK INFORMACYJNYCH

Definicja

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$$

$$\sigma^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

WYDZIAŁ MATEMATYKI I NAUK INFORMACYJNYCH

Definicja

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$$

$$\sigma^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix} = id$$

WYDZIAŁ MATEMATYKI I NAUK INFORMACYJNYCH

$$\begin{pmatrix} A & E & G & I & N & M \\ E & N & I & G & M & A \end{pmatrix}^{-1} = \begin{pmatrix} E & N & I & G & M & A \\ A & E & G & I & N & M \end{pmatrix} =$$

$$\begin{pmatrix} A & E & G & I & N & M \\ M & A & I & G & E & N \end{pmatrix}$$

WYDZIAŁ MATEMATYKI I NAUK INFORMACYJNYCH

Definicja Permutacje cykliczne (Cykle długości k)

$$a_1 \to a_2 \to \ldots \to a_{k-1} \to a_k \to a_1$$

$$(a_1, a_2, a_3, \ldots, a_k)$$

Cykle długości 2 nazywamy transpozycjami.

WYDZIAŁ MATEMATYKI I NAUK INFORMACYJNYCH

Twierdzenie Każda permutacja rozkłada się na iloczyn rozłącznych cykli.

Twierdzenie Każda permutacja rozkłada się na iloczyn rozłącznych cykli.

$$\begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M \\ U & V & X & Y & Z & K & W & A & N & T & B & C & D \end{pmatrix}$$

$$\begin{pmatrix} N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ E & F & G & H & I & J & L & M & O & P & Q & R & S \end{pmatrix}$$

WYDZIAŁ MATEMATYKI I NAUK INFORMACYJNYCH

Twierdzenie Każda permutacja rozkłada się na iloczyn rozłącznych cykli.

$$\begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M \\ U & V & X & Y & Z & K & W & A & N & T & B & C & D \end{pmatrix}$$

$$\begin{pmatrix} N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ E & F & G & H & I & J & L & M & O & P & Q & R & S \end{pmatrix}$$

$$(A, U, M, D, Y, R, I, N, E, Z, S, J, T, L, C, X, Q, H)$$

Twierdzenie Każda permutacja rozkłada się na iloczyn rozłącznych cykli.

$$\begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M \\ U & V & X & Y & Z & K & W & A & N & T & B & C & D \end{pmatrix}$$

$$\begin{pmatrix} N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ E & F & G & H & I & J & L & M & O & P & Q & R & S \end{pmatrix}$$

$$(A, U, M, D, Y, R, I, N, E, Z, S, J, T, L, C, X, Q, H) \circ (B, V, O, F, K)$$

Twierdzenie Każda permutacja rozkłada się na iloczyn rozłącznych cykli.

$$\begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M \\ U & V & X & Y & Z & K & W & A & N & T & B & C & D \end{pmatrix}$$

$$\begin{pmatrix} N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ E & F & G & H & I & J & L & M & O & P & Q & R & S \end{pmatrix}$$

$$(A, U, M, D, Y, R, I, N, E, Z, S, J, T, L, C, X, Q, H) \circ (B, V, O, F, K) \circ (G, W, P)$$

Twierdzenie Każda permutacja rozkłada się na iloczyn transpozycji.

Twierdzenie Każda permutacja rozkłada się na iloczyn transpozycji.

$$\begin{pmatrix} A & E & G & I & N & M \\ E & N & I & G & M & A \end{pmatrix}$$

Twierdzenie Każda permutacja rozkłada się na iloczyn transpozycji.

$$\begin{pmatrix} A & E & G & I & N & M \\ E & N & I & G & M & A \end{pmatrix}$$

$$\begin{pmatrix} A & E & G & I & N & M \\ E & A & G & I & N & M \end{pmatrix}$$

WYDZIAŁ MATEMATYKI I NAUK INFORMACYJNYCH

Twierdzenie Każda permutacja rozkłada się na iloczyn transpozycji.

$$\begin{pmatrix} A & E & G & I & N & M \\ E & N & I & G & M & A \end{pmatrix}$$

$$\begin{pmatrix} A & E & G & I & N & M \\ N & E & G & I & A & M \end{pmatrix} \circ \begin{pmatrix} A & E & G & I & N & M \\ E & A & G & I & N & M \end{pmatrix}$$

Twierdzenie Każda permutacja rozkłada się na iloczyn transpozycji.

$$\begin{pmatrix} A & E & G & I & N & M \\ E & N & I & G & M & A \end{pmatrix}$$

$$\begin{pmatrix} A & E & G & I & N & M \\ A & E & I & G & N & M \end{pmatrix}$$

$$\circ\begin{pmatrix} A & E & G & I & N & M \\ N & E & G & I & A & M \end{pmatrix}\circ\begin{pmatrix} A & E & G & I & N & M \\ E & A & G & I & N & M \end{pmatrix}$$

Twierdzenie Każda permutacja rozkłada się na iloczyn transpozycji.

$$\begin{pmatrix} A & E & G & I & N & M \\ E & N & I & G & M & A \end{pmatrix}$$

$$\begin{pmatrix} A & E & G & I & N & M \\ M & E & G & I & N & A \end{pmatrix} \circ \begin{pmatrix} A & E & G & I & N & M \\ A & E & I & G & N & M \end{pmatrix}$$

$$\circ \begin{pmatrix} A & E & G & I & N & M \\ N & E & G & I & A & M \end{pmatrix} \circ \begin{pmatrix} A & E & G & I & N & M \\ E & A & G & I & N & M \end{pmatrix}$$

WYDZIAŁ MATEMATYKI I NAUK INFORMACYJNYCH

$$\begin{pmatrix} A & E & G & I & N & M \\ E & N & I & G & M & A \end{pmatrix} =$$

$$= \begin{pmatrix} A & E & G & I & N & M \\ M & E & G & I & N & A \end{pmatrix} \circ \begin{pmatrix} A & E & G & I & N & M \\ A & E & I & G & N & M \end{pmatrix}$$

$$\circ \begin{pmatrix} A & E & G & I & N & M \\ N & E & G & I & A & M \end{pmatrix} \circ \begin{pmatrix} A & E & G & I & N & M \\ E & A & G & I & N & M \end{pmatrix}$$

WYDZIAŁ MATEMATYKI I NAUK INFORMACYJNYCH

$$\begin{pmatrix} A & E & G & I & N & M \\ E & N & I & G & M & A \end{pmatrix} =$$

$$= \begin{pmatrix} A & E & G & I & N & M \\ M & E & G & I & N & A \end{pmatrix} \circ \begin{pmatrix} A & E & G & I & N & M \\ A & E & I & G & N & M \end{pmatrix}$$

$$\circ \begin{pmatrix} A & E & G & I & N & M \\ N & E & G & I & A & M \end{pmatrix} \circ \begin{pmatrix} A & E & G & I & N & M \\ E & A & G & I & N & M \end{pmatrix} =$$

$$= (M, A) \circ (G, I) \circ (A, N) \circ (A, E)$$

$$\begin{pmatrix} A & E & G & I & N & M \\ E & N & I & G & M & A \end{pmatrix} =$$

$$= \begin{pmatrix} A & E & G & I & N & M \\ M & E & G & I & N & A \end{pmatrix} \circ \begin{pmatrix} A & E & G & I & N & M \\ A & E & I & G & N & M \end{pmatrix}$$

$$\circ \begin{pmatrix} A & E & G & I & N & M \\ N & E & G & I & A & M \end{pmatrix} \circ \begin{pmatrix} A & E & G & I & N & M \\ E & A & G & I & N & M \end{pmatrix} =$$

$$= (M, A) \circ (G, I) \circ (A, N) \circ (A, E)$$

Uwaga Cykle długości 2 wystepujące w tym rozkładzie nie sa rozłączne.

Twierdzenie 1 Permutacja jest równa swojej odwrotnej wtedy i tylko wtedy, gdy jej rozkład na rozłączne cykle składa sie wyłącznie z cykli długości dwa i jeden.

WYDZIAŁ
MATEMATYKI I NAUK
INFORMACYJNYCH

Twierdzenie 1 Permutacja jest równa swojej odwrotnej wtedy i tylko wtedy gdy jej rozkład na rozłączne cykle składa sie wyłącznie z cykli długości dwa i jeden.

Twierdzenie 2 Załóżmy, że permutacja P zawiera 2-cykle

$$(x_1, y_1)(x_2, y_2) \dots (x_k, y_k),$$

a permutacja Q zawiera 2 cykle

$$(y_1, x_2)(y_2, x_3) \dots (y_k, x_1),$$

wówczas złożenie zawiera QP zawiera k-cykle $(x_1, \dots, x_k)$ oraz $(y_k, \dots, y_1)$.

WYDZIAŁ MATEMATYKI I NAUK INFORMACYJNYCH

Twierdzenie 1 Permutacja jest równa swojej odwrotnej wtedy i tylko wtedy, gdy jej rozkład na rozłączne cykle składa sie wyłącznie z cykli długości dwa i jeden.

Twierdzenie 1 Permutacja jest równa swojej odwrotnej wtedy i tylko wtedy gdy jej rozkład na rozłączne cykle składa sie wyłącznie z cykli długości dwa i jeden.

Twierdzenie 2 Załóżmy, że permutacja P zawiera 2-cykle

$$(x_1, y_1)(x_2, y_2)\ldots(x_k, y_k),$$

a permutacja Q zawiera 2- cykle

$$(y_1, x_2)(y_2, x_3)\ldots(y_k, x_1),$$

wówczas złożenie zawiera QP zawiera k-cykle $(x_1, \ldots, x_k)$ oraz $(y_k, \ldots, y_1)$.

Wniosek Jeśli dwie permutacje składają się tylko z rozłącznych cykli długości 2 to po ich złożeniu wystepują pary cykli rozłącznych o tej samej długości, przy czym elementy tworzące jedną transpozycję w czynnikach wejdą w złożeniu do dwóch różnych cykli.

WYDZIAŁ MATEMATYKI I NAUK INFORMACYJNYCH

Twierdzenie 3 Jeśli w permutacji występuje parzysta liczba cykli rozłącznych tej samej długości, to mozna ją rozłozyć na dwie z których każda jest iloczynem rozłącznych transpozycji.

1	AUQ	AMN	23	NXD	QTU	45	TMN	EBY
2	BNH	CHL	24	NXD	QTU	46	TMN	EBY
3	BCT	CGJ	25	NLU	QFZ	47	TAA	EXB
4	CIK	BZT	26	OBU	DLZ	48	USE	NWH
5	DDB	VDV	27	PVJ	FEG	49	VII	PZK
6	EJP	IPS	28	QGA	LYB	50	VII	PZK
7	FBR	KLE	29	QGA	LYB	51	VQZ	PVR
8	GPB	ZSV	30	RJL	WPX	52	VQZ	PVR
9	HNO	THD	31	RJL	WPX	53	WTM	RAO
10	HNO	THD	32	RJL	WPX	54	WTM	RAO
11	HXV	TTI	33	RJL	WPX	55	WTM	RAO
12	IKG	JKF	34	RFC	WQQ	56	WKI	RKK
13	IKG	JKF	35	SYX	SCW	57	XRS	GNM
14	IND	JHU	36	SYX	SCW	58	XRS	GNM
15	JWF	MIC	37	SYX	SCW	59	XOI	GUK
16	JWF	MIC	38	SYX	SCW	60	XYW	GCP
17	KHB	XJV	39	SYX	SCW	61	YPC	OSQ
18	KHB	XJV	40	SJM	SPO	62	YPC	OSQ
19	LDR	HDE	41	SJM	SPO	63	ZZY	YRA
20	LDR	HDE	42	SJM	SPO	64	ZEF	YOC
21	MAW	UXP	43	SUG	SMF	65	ZSJ	YWG
22	MAW	UXP	44	SUG	SMF			

Rysunek 3.5: Tablica identyfikatorów ENIGMY.

$$P_4P_1 = (B,C)(R,W)(DVPFKXGZYO)(EIJMUNQLHT)(A)(S)$$

$$P_5P_2 = (AXT)(CGY)(BLFQVEOUM)(HJPSWIZRN)(D)(K)$$

$$P_6P_3 = (ABVIKTJGFCQNY)(DUZREHLXWPSMO).$$

WYDZIAŁ MATEMATYKI I NAUK INFORMACYJNYCH