Ukázky aplikací matematiky

Jaro 2014, 2. přednáška

Polsko 1926

Odposlechnuté radiové zprávy Wehrmachtu

- MFNOJ WYFHJ EXZZD BJNDS BECFE NGQOU CFWZE RBSFQ WCUCQ XCKTT RDOAC VDYPM XYOFF HMSOZ THOSD HFPDI UKWRD MNDZX BYMIA FXXTA WWFYS G
- NEVGW YCJUM IYFCW JXMDR TBIFU PQDMH RPCOX WYXTJ YQXZG CQMSP CJHGA OMHEV QFCGX SXATA HXFHV HZBED VALPY ZPMPW JNPDY RZXKJ DDQZO X
- NEVGW YIPUC AVKHH FTAPT ZVYXV KRJIG APWAT LWBQH UJASR JMBSF KDVRN IUOXV FKLQG MPSWY EDYHP LSICW ALFPZ XOOFZ BNZUX DCEKG PXJON U

Všechna písmena se vyskytují přibližně stejněkrát

Frekvence písmen v němčině není rovnoměrná

E	N	I	S	R	. . .	P	J	X,Y,Q
19,2%	10,2%	8,2%	7,1%	7,0%		0,5%	0,16%	0,01%

Identifikace šifry

```
MFNOJ WYFHJ EXZZD BJNDS BECFE NGQOU CFWZE RBSFQ WCUCQ XCKTT
NEVGW YCJUM IYFCW JXMDR TBIFU PQDMH RPCOX WYXTJ YQXZG CQMSP

RDOAC VDYPM XYOFF HMSOZ THOSD HFPDI UKWRD MNDZX BYMIA FXXTA
CJHGA OMHEV QFCGX SXATA HXFHV HZBED VALPY ZPMPW JNPDY RZXKJ

WWFYS G
DDQZO X

NEVGW YIPUC AVKHH FTAPT ZVYXV KRJIG APWAT LWBQH UJASR JMBSF
NEVGW YCJUM IYFCW JXMDR TBIFU PQDMH RPCOX WYXTJ YQXZG CQMSP

KDVRN IUOXV FKLQG MPSWY EDYHP LSICW ALFPZ XOOFZ BNZUX DCEKG
CJHGA OMHEV QFCGX SXATA HXFHV HZBED VALPY ZPMPW JNPDY RZXKJ

PXJON U
DDQZO X
```

Index koincidence němčiny je přibližně 8%.

Pokud je prvních šest písmen u dvou zpráv ve stejný den shodných, pak šifra zachovává index koincidence. **Jde asi o polyalfabetickou šifru**.

Množství zpráv nasvědčovalo, že k šifrování je patrně využíván nějaký přístroj.

Enigma

klávesnice

žárovky

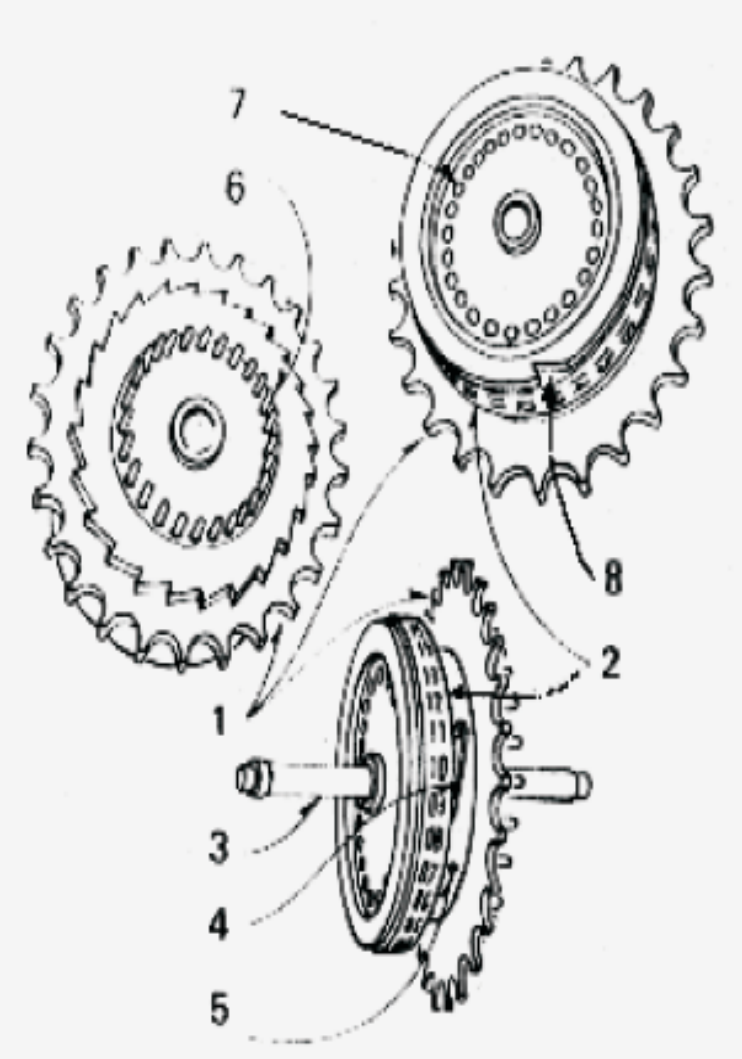
propojovací deska

okénka

ozubená kolečka

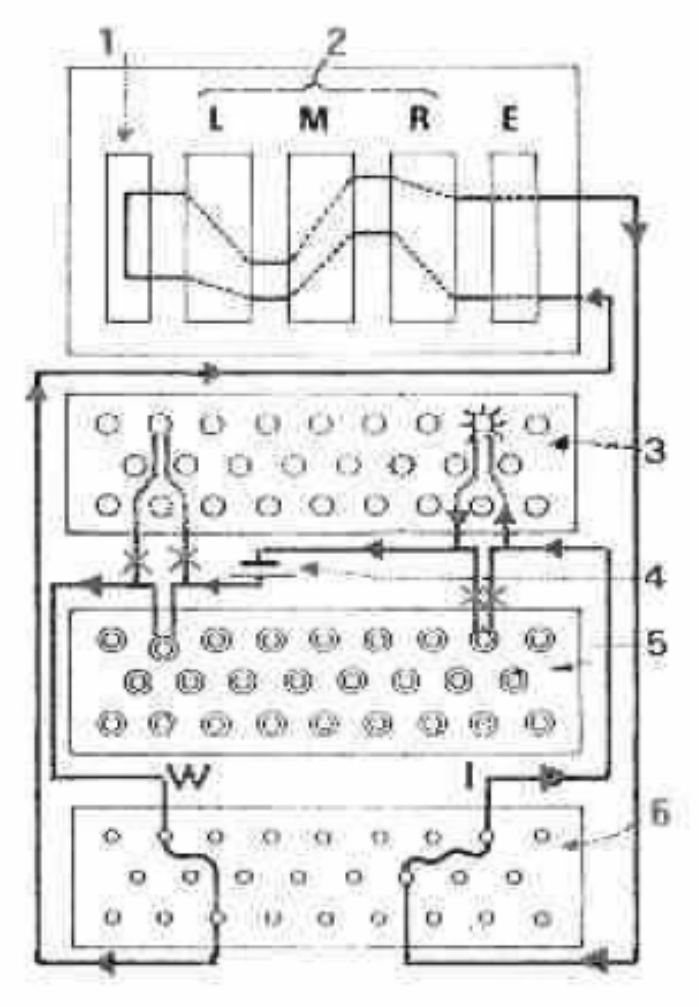
měřič napětí

Rotor



1. ozubené kolečko
2. abecední kroužek
3. společná osa rotorů
4. spona abecedního kroužku
5. tělo rotoru s 26 dráty
6. kontaktní kolíky
7. kontaktní plošky
8. zářez pro přenos pohybu

Elektrické schéma



E - vstupní rotor

1. reflektor
2. trojice rotorů
3. žárovky
4. baterie
5. klávesnice
6. propojovací deska

Manuál pro operátory

- Francouzská špionáž získala manuál pro operátory vojenského přístroje Enigma komcem roku 1931 (generál Gustave Bertrand).
- Německým agentem byl Hans-Thilo Schmidt (1888-1944).
- Později předal francouzské špionáži také denní klíče pro měsíce září a říjen 1932.
- Počátkem prosince 1932 dostalo polské Biuro Szyfrów kopie těchto dokumentů na základě dohody o vojenské spolupráci mezi Polskem, Francií a Velkou Británií.
- V prosinci roku 1932 tak Biuro Szyfrów mělo k dispozici:

- komerční přístroj Enigma (bez propojovací desky a s jinými rotory,
- operační manuál,
- denní klíče pro měsíce září a říjen 1932.

Denní klíče

- Denní klíč říkal, jak má být nastavený přístroj Enigma v daném dni na začátku šifrování libovolné zprávy v daném dni.
- Denní klíč sestával z:

  - pořadí rotorů, např. II, III, I , bylo v té době stejné po celý čtvrt roku,
  - polohy abecedních kroužků na rotorech, např. KUB ,
  - propojení v propojovací desce, např. AU, CR, DK, JZ, LN, PS ,
  - základní nastavení, tj. jaká písmena jsou vidět v malých okénkách, např. UFW .

Klíč zprávy

- Po nastavení přístroje podle denního klíče měla obsluha zvolit náhodnou trojici písmen, kupříkladu `HTS` , to je *klíč zprávy,*
- poté ji napsat dvakrát za sebou, tj. `HTS HTS` ,
- pak tuto šestici zašifrovat pomocí přístroje nastaveného podle denního klíče, výsledkem bylo `NEV GWY` ,
- poté ručně přenastavit rotory tak, aby v okénkách byl vidět klíč zprávy,
- a začít šifrovat samotnou zprávu. Tak například zpráva `AHOJ` byla zašifrována jako `JCRI` .

Celou šifrovou zprávu `NEV GWY JCRI` pak obsluha předala radistovi k odvysílání.

Dešifrování na přijímací straně probíhalo naprosto stejně.

Porušení pravidel bezpečnosti

- Všechny klíče zpráv byly ve stejném dni šifrovány pomocí stejného klíče (stejného nastavení přístroje).
- Každý konkrétní klíč zprávy byl šifrován dvakrát pomocí dvou různých klíčů (tj. různých nastavení přístroje).
- Porušení pravidel bezpečnosti bylo počátkem matematické analýzy šifry. Jak jich využít k prolomení šifry?

Konec roku 1932

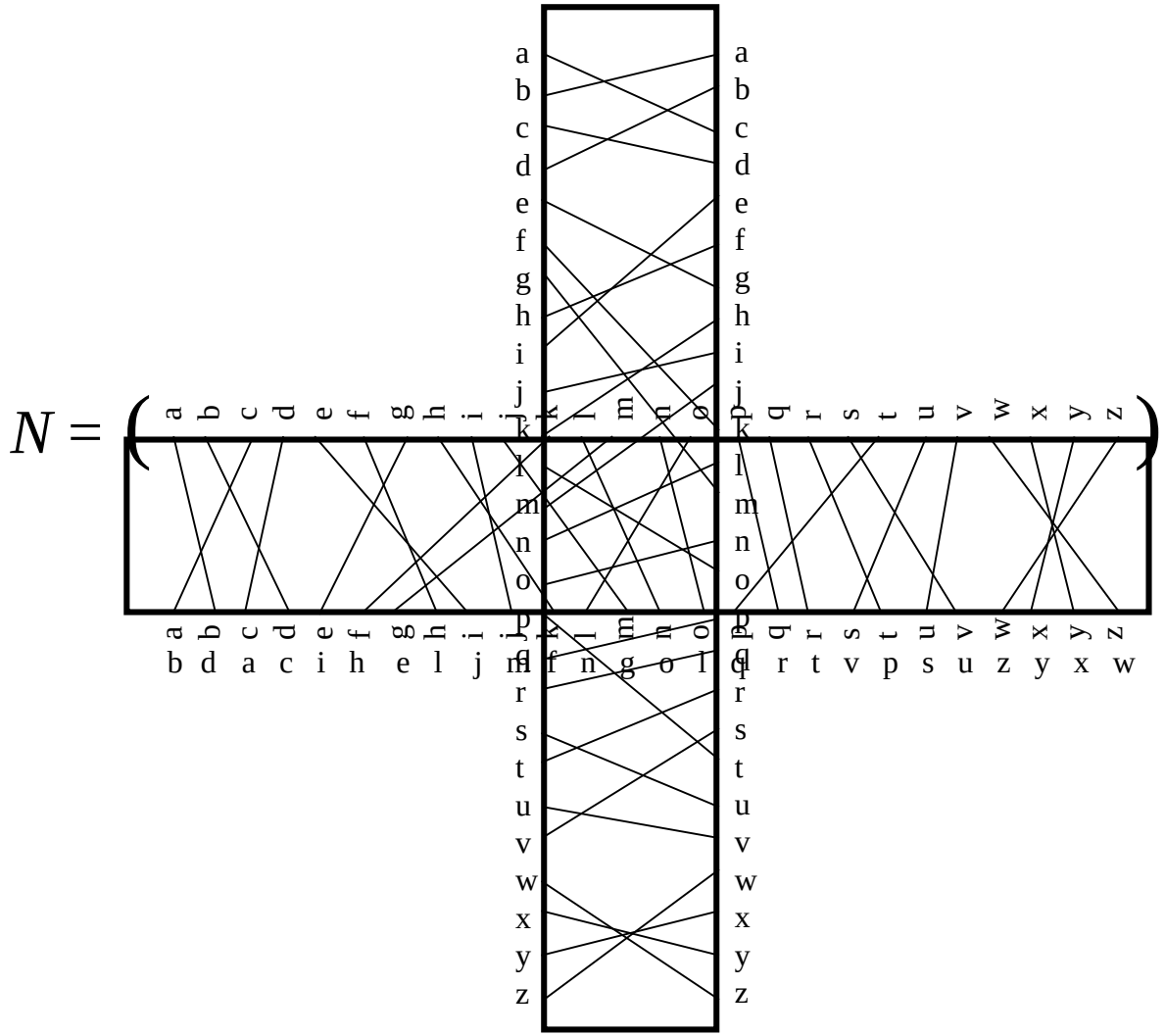
Marian Rejewski
1905-1980

Henryk Zygalski
1906-1978

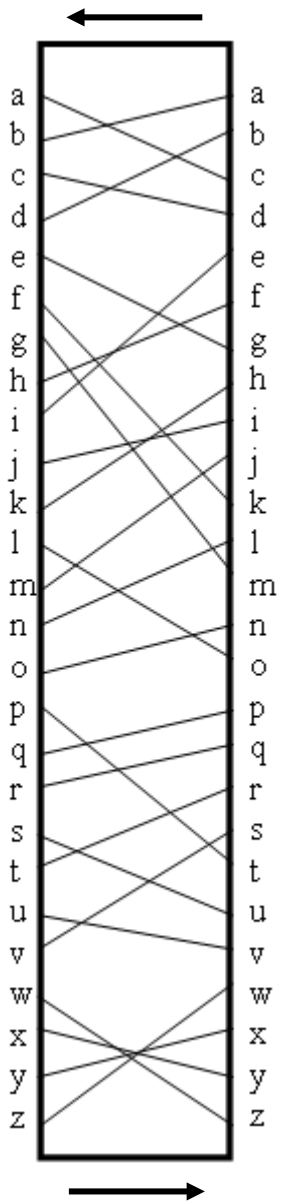
Jerzy Rózycki
1907-1942

Tři nejlepší absolventu kurzu kryptoanalýzy, který uspořádalo Biuro Szyfrów v roce 1928 pro posluchače matematiky na univerzitě v Poznani.

Matematický model rotoru



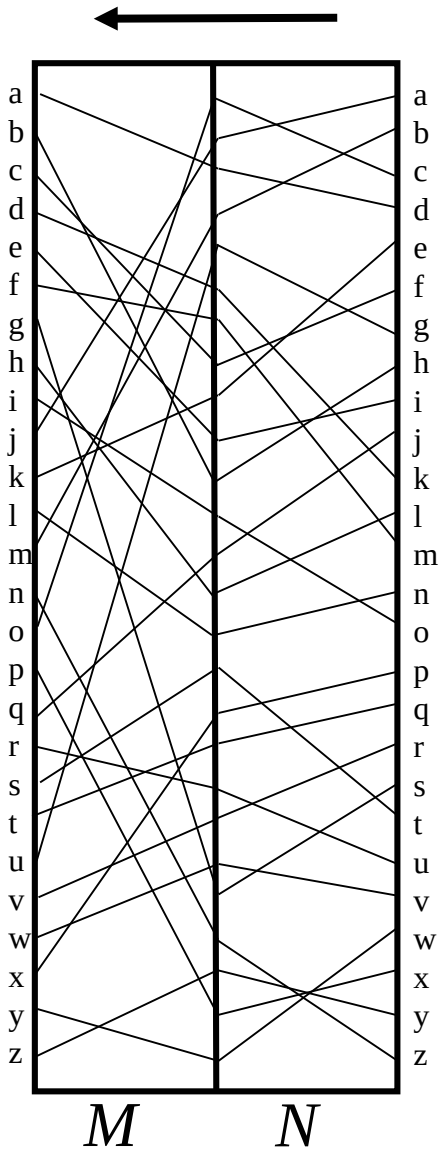
Matematický model rotoru



$$N = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ b & d & a & c & i & h & e & k & j & m & f & n & g & o & l & q & r & t & v & p & s & u & z & y & x & w \end{pmatrix}$$

$$N^{-1} = \begin{pmatrix} b & d & a & c & i & h & e & l & j & m & f & n & g & o & l & q & r & t & v & p & s & u & z & y & x & v \\ a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \end{pmatrix}$$

Rotory lze násobit



$$N: \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ b & d & a & c & i & h & e & k & j & m & f & n & g & o & l & q & r & t & v & p & s & u & z & y & x & w \end{pmatrix}$$

$$M: \begin{pmatrix} b & d & a & c & i & h & e & k & j & m & f & n & g & o & l & q & r & t & v & p & s & u & z & y & x & w \\ j & m & o & a & k & c & u & b & e & q & d & h & f & l & i & x & t & v & g & s & r & w & y & p & z & n \end{pmatrix}$$

$$MN: \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ j & m & o & a & k & c & u & b & e & q & d & h & f & l & i & x & t & v & g & s & r & w & y & p & z & n \end{pmatrix}$$

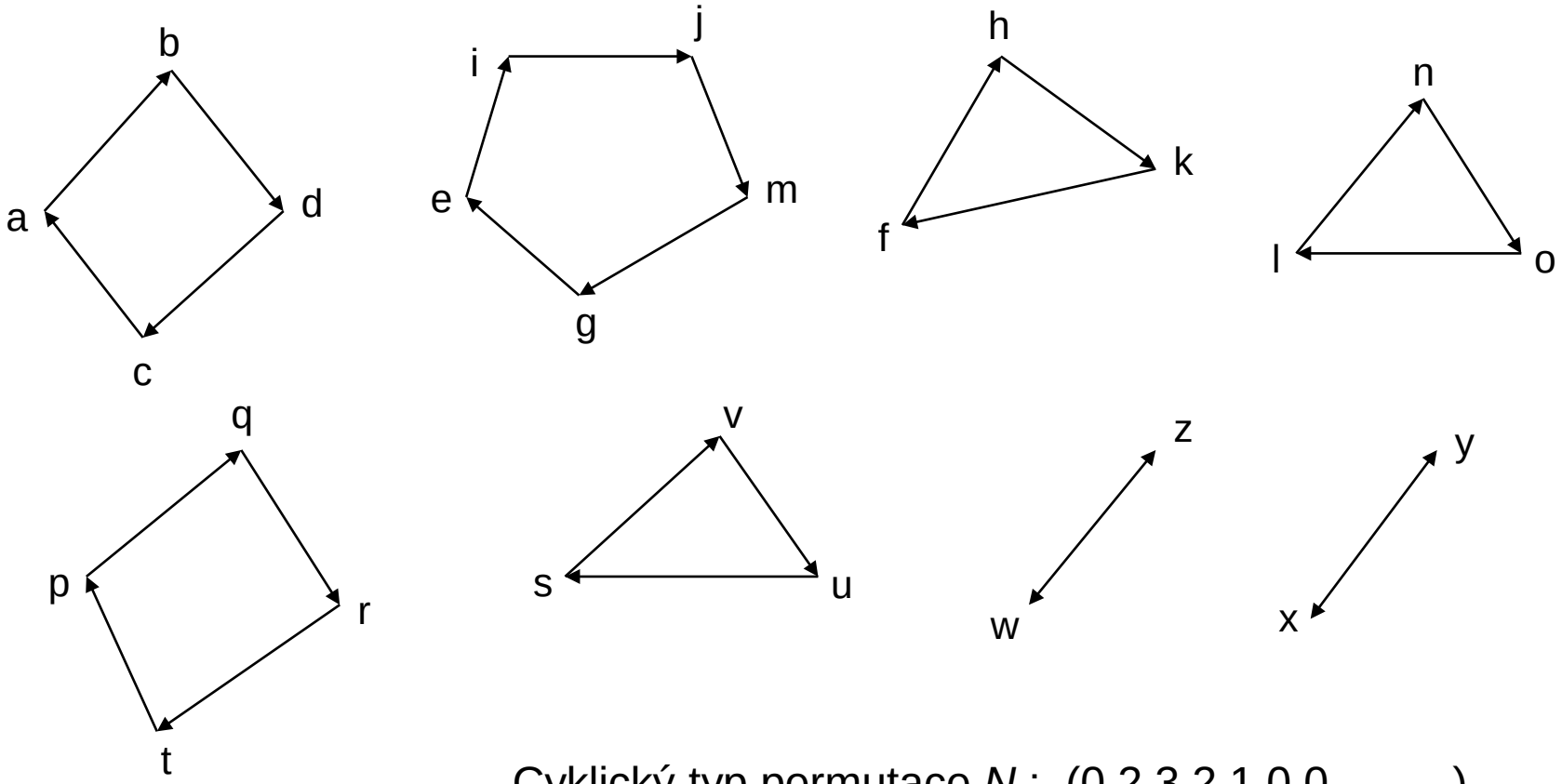
$$NM: \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ l & m & b & g & s & c & h & a & f & i & d & j & r & k & n & v & y & p & t & u & z & e & o & w & q & x \end{pmatrix}$$

MN **se nerovná** NM

$$R(MN)=(RM)N=RMN$$

Grafické znázornění permutací

$$N = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ b & d & a & c & i & h & e & k & j & m & f & n & g & o & l & q & r & t & v & p & s & u & z & y & x & w \end{pmatrix}$$



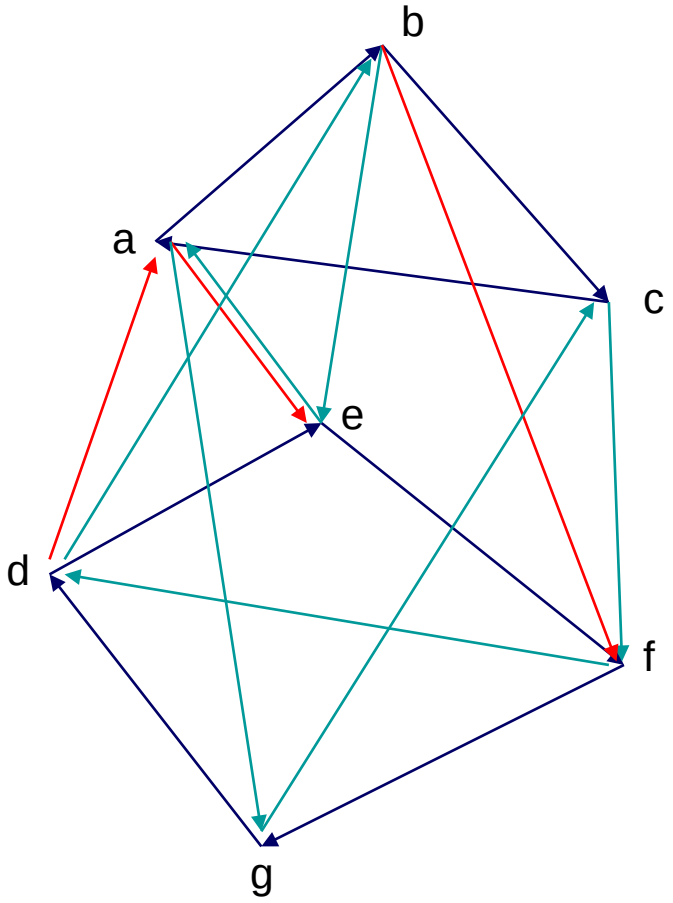
Cyklický typ permutace *N* : (0,2,3,2,1,0,0, ...)

Graf složené permutace

$$N = \begin{pmatrix} a & b & c & d & e & f & g \\ b & c & a & e & f & g & d \end{pmatrix}$$

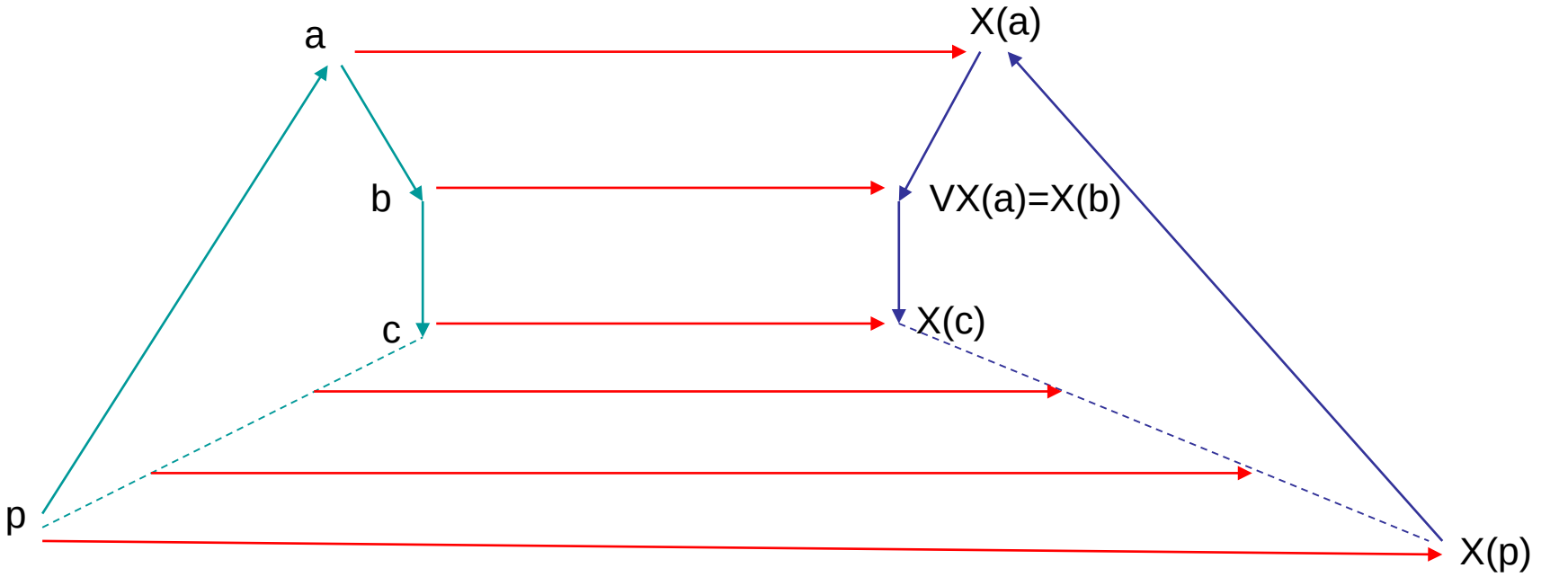
$$M = \begin{pmatrix} b & c & a & e & f & g & d \\ e & f & g & a & d & c & b \end{pmatrix}$$

$$MN = \begin{pmatrix} a & b & c & d & e & f & g \\ e & f & g & a & d & c & b \end{pmatrix}$$



Řešitelnost rovnice $U=X^{-1}VX$

U,V jsou permutace na nějaké množině Z a nechť permutace X na množině Z je řešením této rovnice.



Je-li X řešením rovnice, zobrazuje šipky libovolného cyklu permutace U na šipky nějakého cyklu permutace V téže délky.

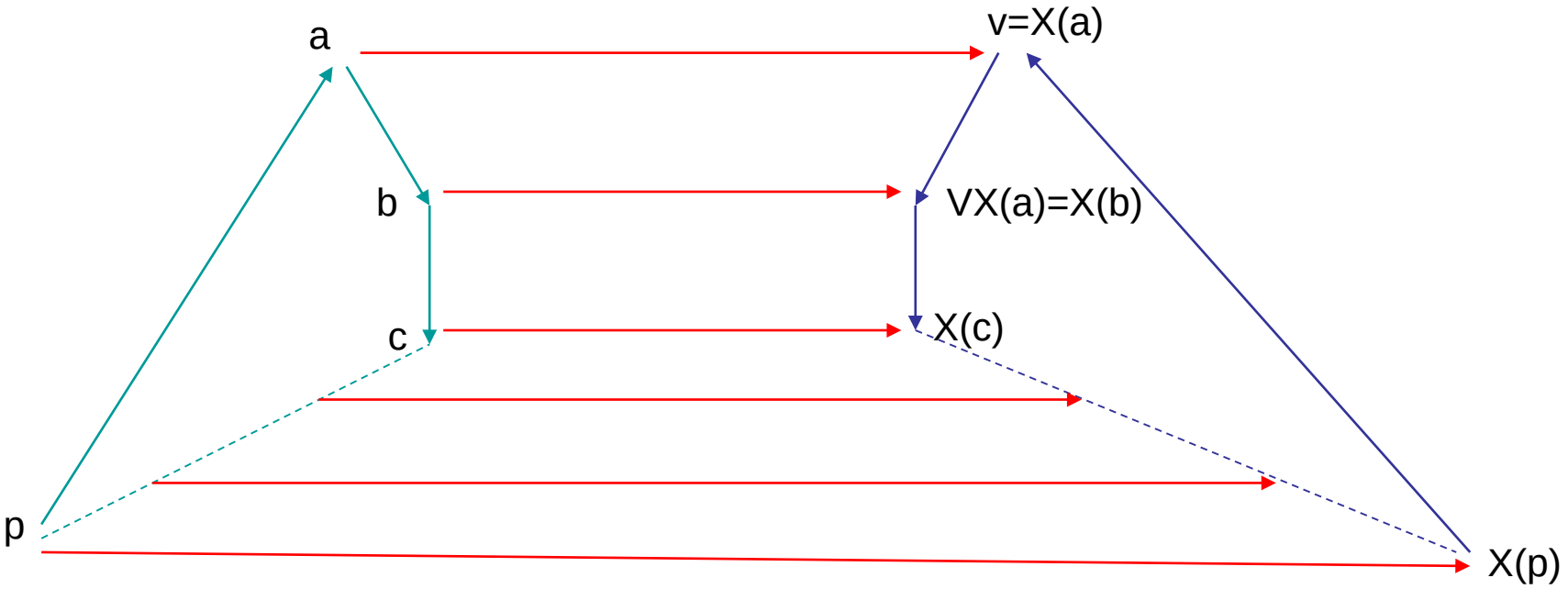
Nutnou podmínkou pro řešitelnost rovnice je to, že permutace U,V musí mít stejný cyklický typ, tj. stejný počet cyklů libovolné délky.

Řešitelnost rovnice $U=X^{-1}VX$

Nechť naopak permutace U,V mají stejný cyklický typ.

Zvolíme nějaký cyklus v permutaci U v nějaký cyklus téže délky v permutaci V.

Dále zvolíme ve vybraném cyklu permutace U prvek a a ve vybraném cyklu permutace V nějaký prvek v a zkusíme najít řešení X, pro které platí $X(a)=v$.



Zvolená hodnota $X(a)$ tak jednoznačně určuje hodnoty permutace X ve všech bodech vybraného cyklu permutace U.

Protože permutace U,V mají stejný permutační typ, můžeme spárovat cykly permutace U s cykly permutace V stejné délky.

Řešitelnost rovnice $U=X^{-1}VX$

Platí proto následující tvrzení. Říká se mu *věta o konjugovaných permutacích*.

Věta. Jsou-li U,V dvě permutace na konečné množině Z, pak existuje permutace X na množině Z, pro kterou platí, že $U=X^{-1}VX$ právě když permutace U,V mají stejný cyklický typ.

Uvedený nástin důkazu ve skutečnosti obsahuje algoritmus, jak najít všechna řešení této rovnice.

Každý pár cyklů délky n dává n možností, jak permutaci X definovat na prvcích toho cyklu permutace U, který v daném páru leží.

Leží-li v každé z permutací U,V právě $k=p_n$ cyklů délky n, pak pro dané spárování těchto cyklů dostaneme celkem n^k možností, jak definovat permutaci X na prvcích cyklů délky n.

A protože možných spárování k cyklů je $k!$, celkový počet počet možností, jak definovat permutaci X na k cyklech délky n, je $k! \times n^k$.

Celkový počet řešení X je pak součinem těchto čísel přes všechny délky cyklů n.

Počet řešení

Například, mají-li U,V po jednom cyklu délky 26, pak má rovnice 26 řešení.

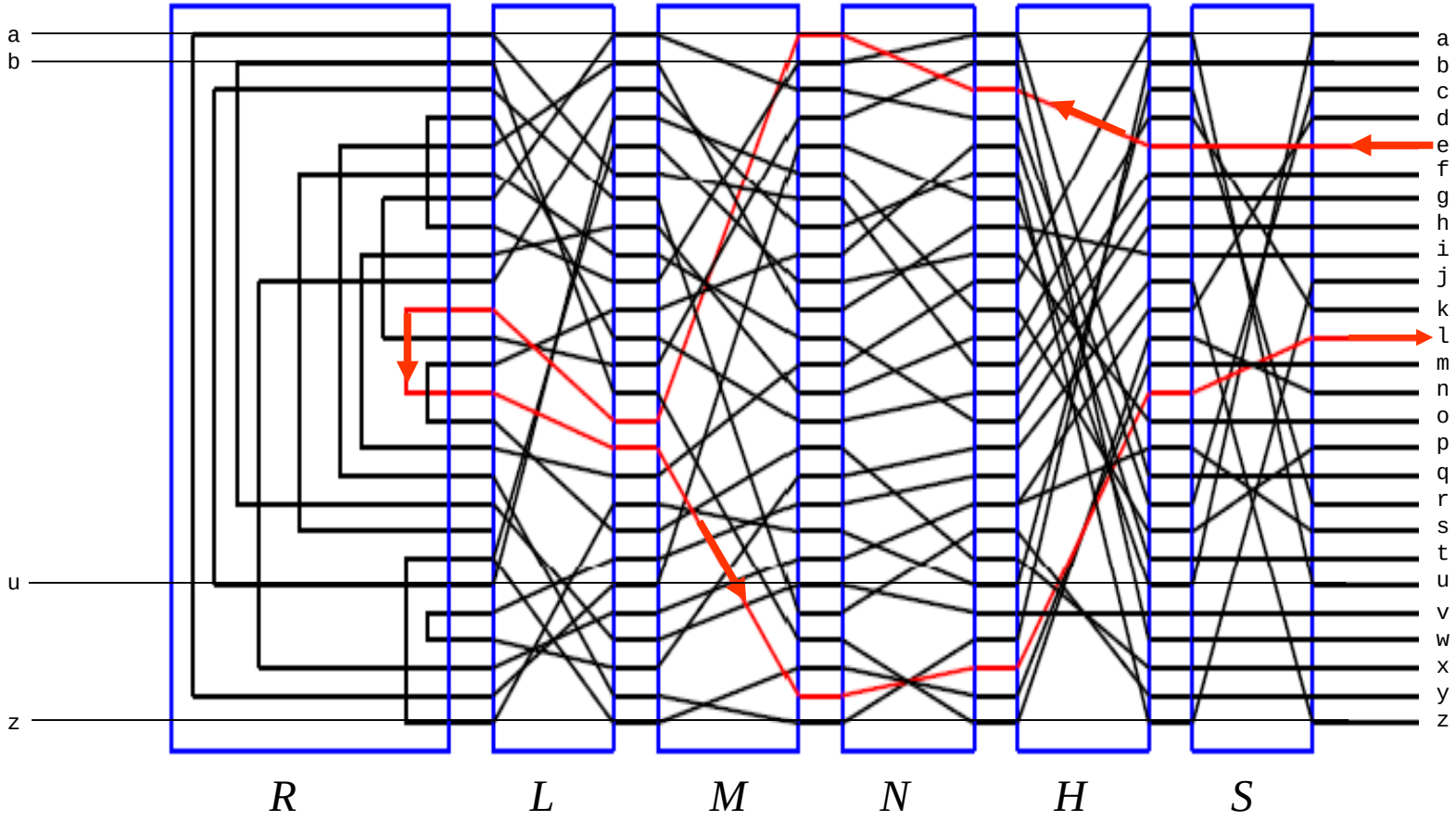
Mají-li U,V po dvou cyklech délky 13, pak má rovnice $2 \times 13^2 = 338$ řešení.

Mají-li U,V cyklický typ (0,2,3,2,1,0,0, ...), pak počet řešení rovnice $U = X^{-1}VX$ je

$$(2! \times 2^2) \times (3! \times 3^3) \times (2! \times 4^2) \times 5 \ .$$

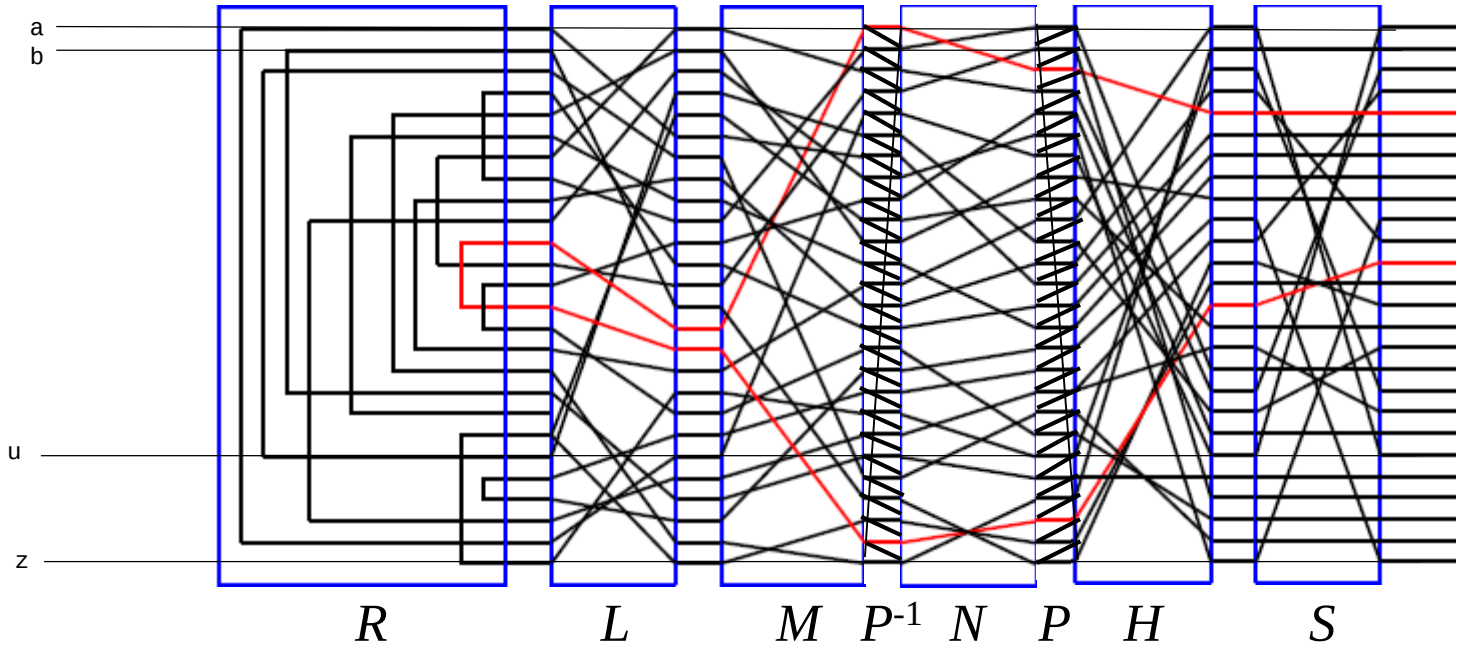
Mají-li U,V cyklický typ (26,0,0,0,0, ...), pak má rovnice 26! řešení, neboť každá permutace X je řešením.

Statický model



$$S^{-1}H^{-1}N^{-1}M^{-1}L^{-1}RLMNHS$$

Dynamický model



$$P = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z & a \end{pmatrix}$$

$$A = S^{-1}H^{-1}P^{-1}N^{-1}PM^{-1}L^{-1}RLMP^{-1}NPHS$$