RUMACJEPET

MTACJEPERU

PTACJEEMUR

MATCJEPERU

PTACEMURJE

PERMUTACJE

PERUMTACJE

EMURPTACJE

MTPERUACJE

PTACJEUREM

RUMATCJEPE

Krzysztof Kotarski

Szymon Nowak

Filip Zieliński

Dawid Żuk

WSTĘP

Wiedza o permutacjach nie jest zbyt powszechna w szkole podstawowej. Może właśnie dlatego, że informacje te były dla nas nowe zdobywanie ich i coraz lepsze rozumienie tematu stało się tak fascynujące. Zachęceni przez nauczycieli postanowiliśmy napisać swoją pierwszą pracę matematyczną. Ktoś, kto interesuje się matematyką, przeczytawszy nasz referat, może dowiedzieć się o permutacjach czegoś nowego. Oczywiście rozpoczynamy od znanych wiadomości teoretycznych. W kolejnych rozdziałach jednak poruszamy wiadomości związane z działaniami na permutacjach czy temat związany z permutacjami chaotycznymi i lingwistycznymi (nowy nawet dla ludzi interesujących się matematyką). Na koniec prezentujemy historyczne zastosowanie permutacji w rozwiązaniu szyfru Enigmy.

Mamy nadzieję, że po wykonaniu przygotowanych przez nas zadań bez problemu opanujecie podstawy permutacji. Pisząc ten wstęp, chcieliśmy również podziękować pani Annie Ochel i wykładowcom z programu Eksploratorium Twórczej Matematyki z Uniwersytetu Pedagogicznego w Krakowie, bez których napisanie tej pracy byłoby niemożliwe. Prawdę mówiąc byli Oni naszym jedynym źródłem rzetelnych informacji w tej dziedzinie. Permutacje nie są łatwym działem matematyki, ale teraz możemy stwierdzić, że ich znajomość ułatwia zrozumienie pewnych innych zagadnień szczególnie z rachunku prawdopodobieństwa. Z pewnością są nietypowe. Czasami mogłoby się wydawać, że są dziwolągiem matematycznym.

Serdecznie zapraszam na lekcję matematyki, inną niż wszystkie. Przedstawiamy Wam naszą wiedzę o permutacjach.

1!

Rozpocznijmy od wprowadzenia definicji pojęcia kluczowego.

***Permutacja*** *to przestawienie elementów zbioru skończonego.*

Liczbę permutacji (*Pn*) zbioru *n* elementowego obliczamy ze wzoru

*Pn = n!*

gdzie *n!* (czytamy *n silnia*) oznacza iloczyn liczb od *1* do *n*.

Dla lepszego zrozumienia przeanalizujmy powyższe pojęcia na przykładzie.

Weźmy zbiór 4-ro elementowy {1,2,3,4}. Permutacją tego zbioru będzie zatem (2341), (4321) lub (3142). Wszystkich permutacji tego zbioru będzie

P4  = 4! = 1 . 2 . 3 . 4=24

Dość dużo jak na cztery elementy. Jak łatwo obliczyć, jeżeli dodamy piąty element permutacji będzie już 120.

W różnych opracowaniach matematycznych natrafiłem na wiele sposobów samego zapisu permutacji.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| (1234) | 1 2  2 3  3 4  4 1 | 1 2 3 4  2 3 4 1 |  | ( 2,3,4,1) |

Zapisywanie permutacji za pomocą strzałek jest mało wygodny, dlatego częściej używamy ***cykli*** , czyli zapisu z piątej kolumny. Zapis ( 2,3,4,1) oznacza:

2 3

3 4

4 1

1. 2

Wszystkie cyfry zmieniane są w cykliczny sposób na kolejną cyfrę, a ostatnia w nawiasie jest zmieniana na pierwszą. Permutację, która niczego nie przestawia, zapisujemy za pomocą symbolu i nazywamy ***identycznością***. W swojej pracy będę używał różnego zapisu.

Jeżeli dobrze już zrozumiałeś definicje permutacji to możesz przejść do następnego rozdziału. Jeżeli chciałbyś sprawdzić jak radzisz sobie samodzielnie z omawianym materiałem to wykonaj zadania ze strony 20.

2!

Permutacje można ze sobą łączyć za pomocą iloczynu, który oznaczać będziemy \*.

Na przykład: zapis (1,2,4) (1,3) oznacza

1 2 1 3

2 4 a potem 2 2

3 3 3 1

4 1 4 4

Pierwszy ruch rozpisujemy z pierwszego z cyklu, natomiast drugi ruch rozpisujemy z drugiego cyklu. A zatem otrzymujemy

1 2 2

2 4 4

3 3 1

4 1 3

Możemy to zapisać następująco:

(1,2,4) \* (1,3) = (1,2,4,3)

W tym przypadku iloczyn dwóch cykli okazał się dłuższym cyklem. Jednak nie zawsze tak jest.

Przykład:

(2,5,3) \* (2,4,3) = (2,5) \* (3,4)

W tym przypadku iloczyn cykli w ogóle nie jest cyklem

Twierdzenie 1. *Iloczyn permutacji nie jest**przemienny.*

(1,2,4) \* (1,3) (1,3) \* (1,2,4)

Jest wiele metod na mnożenie czy też składanie permutacji. Zaprezentujemy jedną z ciekawszych i dosyć prostych do opanowania. Permutacje mnożymy od prawej do lewej, co wynika z ogólnie przyjętego zapisu składania funkcji, którymi de facto są permutacje, ale tym nie będziemy się głębiej zajmować. Złóżmy następujące permutacje:

Nazwijmy permutację po lewej stronie „*A*”, a tą po prawej „*B*”. Trzeba pamiętać, że mnożymy B\*A, a nie A\*B, mnożenie permutacji nie jest przemienne. Metoda polega na tym aby pod permutacją B zapisać permutacje A, ale pozamieniać kolumny w taki sposób aby dolny wiersz B i górny A był identyczny, trzeba przy tym pamiętać aby obrazy dolnego wierszu A odpowiadały jego argumentom. Będzie to wyglądało następująco:

Teraz aby otrzymać wynik składania bierzemy górny wiersz B i dolny wiersz A, czyli naszym rozwiązaniem jest:

***Rzędem cyklu*** nazywamy minimalną liczbę powtórzeń tego cyklu, którą należy wykonać aby otrzymać identyczność.

Rząd cyklu (2,3,4) wynosi 3.

2 3 4 2 3 4 2 3 4 2 3 4

Twierdzenie 2*. Rząd cyklu jest równy liczbie elementów tego cyklu.*

***Rzędem permutacji*** nazywamy minimalną liczbę powtórzeń tej permutacji potrzebną, aby otrzymać identyczność.

Rząd permutacji (2,3) \* (4,5,6,7) wynosi 4.

2 3 3 2 2 3 3 2 2 3 2 2 3 3 2 2 3 3 4 4 5 5 6 6 7 7 4 5 5 6 6 7 7 4 4 5 6 6 7 7 4 4 5 5 6 7 7 4 4 5 5 6 6 7

1 ruch 2 ruch 3 ruch 4 ruch

Dwa cykle nazywamy ***rozłącznymi*** gdy nie mają one wspólnych elementów.

Cykle (1,3) i (2,4) są rozłączne, ponieważ nie mają wspólnych elementów.

Cykle (1,3) i (1,2) nie są rozłączne, ponieważ mają jeden wspólny element (1).

Twierdzenie 3*. Rząd iloczynu cykli rozłącznych jest równy najmniejszej wspólnej wielokrotności rzędu tych cykli.*

Jak zatem obliczyć rząd iloczynu cykli, które nie są rozłączne ?

W pierwszej kolejności zamieniamy cykle nie rozłączne na cykle rozłączne oraz obliczamy ich rzędy. Zobrazujmy to przykładem

(2,4,3,1) (2,4,5) = (1,4,3) (2,5)

Rząd cyklu (2,5) wynosi 2.

Rząd cyklu (1,4,3) również wynosi 3.

W związku z tym, najmniejsza wspólna wielokrotność rzędów cykli (2,5) i (1,4,3) wynosi 6. Tak więc rząd iloczynu tych cykli również wynosi 6.

Jeżeli możemy permutacje mnożyć to jak wygląda potęgowanie?

Ponownie przeanalizujemy to na przykładzie permutacji

2 =

3 = =

Każda permutacja jest przestawieniem elementów zbioru *n* elementowego. Można zatem wskazać ***przestawienie odwrotne***, czyli takie w wyniku którego elementy „wrócą” na swoje miejsca. Permutacje i są odwrotne, jeśli .  =

Permutację odwrotną do zapisujemy jako  -1

Zatem dla =  -1 =

Przykłady:

= =

=

Zachęcam teraz czytelników do rozwiązania zadań to tego rozdziału znajdujących się na stronie 20.

3!/2

Permutacja odwrotna jest zatem rozwiązaniem równania .

X = .

Równanie to, zawsze ma dokładnie jedno rozwiązanie .

Zatem weźmy proste równanie liniowe A X = B. Jego rozwiązaniem jest

X = A-1 B .

Rozwiązaniem równania

X =

jest permutacja

X = -1  = = = (1,3,2)

Rozwiązaniem równania

X =

jest iloczyn cykli

X = -1  = = = (1,2) (3,4)

4!/3!

Znamy już działanie \*. Jest ono jedynym znanym i opisywanym działaniem na permutacjach. Poszukiwaliśmy nowego działania. Okazało się to nie łatwą sprawą zdefiniować działanie, które miałoby sens. Ostatecznie zaproponowaliśmy .

Jeżeli przemnożymy dwa cykle uporządkujemy je i wyjdzie nam, że dwie lub więcej liczb przeszło na same siebie, to zamieniamy najbliższą, która też nie permutowała w efektywny sposób np.

(1,2) (1,2,3)=

W tym przykładzie w efektywny sposób nie permutowały nam dwie liczby 2 i 4 więc zamieniamy je ze sobą.

Kiedy otrzymamy nieparzystą ilość tych liczb to zamieniamy je ze sobą od najmniejszej do największej np.

(2,3,5) (2,5)=

Nie permutowały tu trzy liczby 1,4 i 5 wiec zamieniamy je ze sobą .

Naturalnym wydaje się poszukanie odpowiedzi na pytanie czy działanie jest przemienne? Odpowiedź jest negatywna co można zaobserwować na poniższym przykładzie.

(2,3,4) (4,2)=(1,4) (3,2)

(4,2) (2,3,4)=(1,2) (3,4)

Teraz możemy spróbować działać tak aby otrzymać identyczność.

(2,3) (4,2)

4 4 21

2

3

Ponownie odpowiedź negatywna. Zatem nasze działanie nie jest specjalnie ciekawe pod względem matematycznym. Będziemy szukali dalej ☺

5!/24

Wiemy już, jak obliczyć liczbę permutacji zbioru n-elementowego.

Na przykład dla zbioru 3-elementowego liczba permutacji będzie wynosiła 6. Co ciekawe, te 6 permutacji możemy podzielić na różne grupy :

1. Permutacja identyczności, czyli taka, w której nie zachodzą żadne zmiany :

1. Permutacje, w których zachodzi n zmian, ale przynajmniej jeden element pozostaje na swoim miejscu. W zbiorze 3 elementowym możemy wyróżnić 3 takie przypadki :

1. Permutacje, w których wszystkie elementy zmieniają swoje miejsca nazywamy ***permutacjami chaotycznymi***. Tymi permutacjami będziemy się zajmować w tym rozdziale. W zbiorze 3 elementowym możemy wyróżnić 2 takie przypadki :

W tych przykładach widzimy, że wszystkie liczby zmieniają swoje położenie. O ile, w zbiorach trzy lub czteroelementowych możemy rozpisać wszystkie permutacje i sprawdzić ile z nich jest chaotycznymi, to w liczniejszych zbiorach jest to bardzo uciążliwe.

Dlatego właśnie poznaliśmy działanie zwane ***przedsilnią*** (nie wiemy kto jest jego autorem). Będziemy oznaczać je znakiem „!n”. Za pomocą przedsilni będziemy obliczać liczbę permutacji chaotycznych w większych zbiorach.

Wzór na obliczenie liczby chaotycznych permutacji w danym zbiorze:

-

+ Dla zbioru 1- elementowego

Dla zbioru 2 - elementowego

+ Dla zbioru 3- elementowego

- … Dla zbioru 4 - elementowego

Przy kolejnych liczbach, nasz wzór będzie się rozszerzał w następujący sposób. Za każdym razem wzór zaczynamy od odejmowania, a potem dodajemy następny segment, i tak na przemian. Zależy to, od tego czy dany segment jest dla liczby parzystej bądź nieparzystej.

Obliczymy ile jest permutacji chaotycznych dla zbiorów 4 i 5 – elementowych.

-

+

+

= 9

-

+

= 44

Dla zbioru 4-elementowego jest ich 9 a dla 5 – elementowego 44.

|  |  |  |
| --- | --- | --- |
| Liczba elementów | n! | !n |
| 3 | 6 | 2 |
| 4 | 24 | 9 |
| 5 | 120 | 44 |

Na podstawie naszych dotychczasowych obliczeń, możemy wyprowadzić łatwiejszy wzór na obliczenie liczby permutacji chaotycznych w danym zbiorze. Posłużymy się metodą ***rekurencyjną.*** Oto następujący wzór :

C(n+1) = n[C(n-1)+C(n)]

Gdzie ***C*** oznacza permutacje chaotyczną.

Przeanalizujmy nasz wzór na zbiorze 3 - elementowym:

Pod n podstawiamy 2.

C(2+1) = C(3) = 2[C(2-1)+C(2)] = 2[0+1]= 2

Tym samym potwierdzamy, że liczba permutacji chaotycznych w zbiorze 3 – elementowym wynosi 2. Gdy będziemy chcieli obliczyć za pomocą naszego wzoru liczbę permutacji chaotycznych dla coraz większych zbiorów, będziemy musieli wziąć pod uwagę jeszcze jedną rzecz. Jeśli chcemy obliczyć liczbę PC dla zbioru np. 56 – elementowego musimy znać liczbę PC zbioru 55 – elementowego. A jeżeli chcemy obliczyć liczbę PC zbioru 55 – elementowego, musimy znać liczbę PC dla zbioru 54 – elementowego, itd. Dlatego w związku tym, chcąc obliczyć liczbę PC dla danego zbioru, musimy najpierw obliczyć liczbę PC dla wszystkich poprzedzających tę liczbę, zbiorów.

Przykład obliczeń dla zbioru 4 i 5 elementowego

C(3+1) = 3[C(3-1)+C(3)] = 9

C(4+1) = 4[C(4-1)+C(4)] = 44

6! - 714

Kolejnym naszym autorskim pomysłem są ***permutacje lingwistycznie właściwe***. Każde słowo to jakiś zbiór liter, a skoro tak to możemy go również permutować. Zatem permutacje lingwistycznie właściwe to zbiór istniejących słów w danym jęzuku w którym każde słowo jest permutacją każdego innego słowa z tego zbioru,

Jeżeli będziemy pisać że jakieś słowo jest permutacją lw. oznacza to po prostu to że jest elementem zbioru jakiejś permutacji lw. Będziemy po porstu używać tego zapisu po to żeby tekst był krótszy.

Będziemy również korzystać z określeń takich jak :

***Singiel***- słowo, które w tekście nie ma żadnych permutacji lw (lingwistycznie właściwych)

***Duet*** – słowo, które w tekście ma dokładnie 1 słowo, które jest jego permutacją

***Tercet*** – słowo, które w tekście ma dokładnie 2 słowa, które są jego permutacjami

***Kwartet*** - słowo, które w tekście ma dokładnie 3 słowa, które są jego permutacjami

***Kwintet*** – słowo, które w tekście ma dokładnie 4 słowa, które są jego permutacjami

Przeanalizujmy więc słowo „tak” w różnych językach pod kątem permutacji lw. Permutacje lw. będziemy oznaczać kolorem czerwonym dla wyróżnienia. Słowo „tak” jest zbiorem 3-elementowym więc wszystkich permutacji jest 6 ale tylko 4 to permutacje lw.

TAK TKA KTA KAT AKT ATK

W języku angielskim jest tylko jedna taka permutacja lw.

YES YSE SEY SYE EYS ESY

Natomiast w języku greckim 2 na 6 permutacji to permutacje lw.

Ναί ίnα ίαn nία αnί αίn

W języku walijskim za to aż 2 na 2 możliwości są permutacjami lw.

IE EI

Jeżeli jesteście ciekawi co oznaczają czerwone słowa w języku greckim i walijskim to zajrzyjcie na koniec pracy do odpowiedzi.

Zachęcamy również do znalezienia permutacji lingwistycznie właściwych z liter W,A,Y,T,R.

Słowo „tak” w większości języków składa się z niewielu liter. Postawiliśmy sobie zatem pytanie przy jakiej długości słów występuje najwięcej permutacji lw?

Żeby rozpatrywać ten problem musimy rozróżnić dwie rzeczy, czyli czy wynik podajemy procentowo czy ilościowo. Jeśli chodzi o procenty to zdecydowanie wygrywają słowa 2,3 literowe bo często się zdarzają ( tak jak np. w słowie tak po walijsku). Skoro istnieje mało kombinacji to nawet jeśli nie jest tych permutacji lw. jakoś dużo to i tak procentowo wychodzi spora liczba. Jeżeli natomiast rozpatrujemy ilościowo to przewagę zyskują słowa 4,5 literowe, których jest dużo więcej więc jest spora szansa na trafienie, że takie słowo istnieje, a też jest dużo więcej ułożeń możliwych niż w przypadku słów 2 i 3 literowych ( w 4 literowych 24 możliwości ułożeń w 5 literowych 120 możliwości ułożeń). Jednocześnie dalej, przy słowach 6,7 literowych jest znowu mniej bo takich słów po prostu nie ma już tak wiele.

Postanowiliśmy wykorzystać sztuczną inteligencję i stworzyliśmy program komputerowy, który wyszukuje i podaje nam wszystkie permutacje lw. w podanym mu tekście. Rozważmy na początek zdanie w języku angielskim. Na pierwszy ogień weźmiemy wszystkim znany tekst – „ The Adventures of Sherlock Holmes” napisany przez Arthur Conana Doyle’a.

W tym tekście jest dokładnie 105310 słów 8348 różnych słów oraz 270 wszystkich permutacji lw.

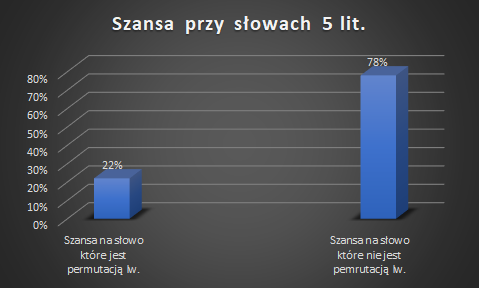
Najwyższa ilość permutacji to kwartet. Są dokładnie 3 takie przypadki z czego 2 są ze słów 4 literowych a 1 z 5 literowego.

Najdłuższe słowa, które są permutacjami lw. to słowa 10 literowe, są takie 2 przypadki.

impression --- permission directions --- discretion

Jeżeli wybierzemy losowe słowo z Sherlocka to mamy 12,78% szansy na to, że to słowo jest permutacją lw. innego słowa w tym tekście. Dokładne dane widać poniżej.

Jeżeli natomiast wykluczymy wszystkie powtórzenia słów to szanse są dużo mniejsze, a dokładnie takie: ( podane w promilach)

Jeżeli w Sherlocku, wybierzemy dowolne słowo 5 literowe szanse na , że to słowo jest permutacją lw. ( w zaokrągleniu) są następujące:

Przy słowach 4 literowych statystyka ta, przedstawia się ciekawie. Otóż samych permutacji lw. słów 4 literowych jest w Sherlocku faktycznie więcej niż przy 5 literowych, ale nie wiele. Za to ogólnie słów 4 literowych jest dużo więcej. Warto też zauważyć, że wiernie pokrywa się z wykresem dla każdej długości słów gdzie to wynosiło trochę ponad 12% (można to zaobserwować na pierwszym wstawionym wykresie). Wykres dla słów 4 literowych (w zaokrągleniu):

Zostawmy już Sherlocka, dla odmiany zajmijmy się teraz tekstem polskim, czyli Krzyżakami autorstwa Henryka Sienkiewicza. Nie będziemy robili bardzo zaawansowanych statystyk po prostu przypatrzmy się liczbom i trochę pobawmy się możliwościami. W krzyżakach jest 226646 wszystkich słów natomiast różnych już tylko 30580. Wszystkich permutacji jest 774, w tym dwa kwartety. Najdłuższą permutacją lw. są dwie permutacje 13 literowe czyli:

wypowiedzenia --- wypowiedziane

przewiązanymi --- przywiązaniem

Jeżeli wybierzemy dowolne słowo w Krzyżakach szansa na to, że jest ono permutacją lw. wynosi:

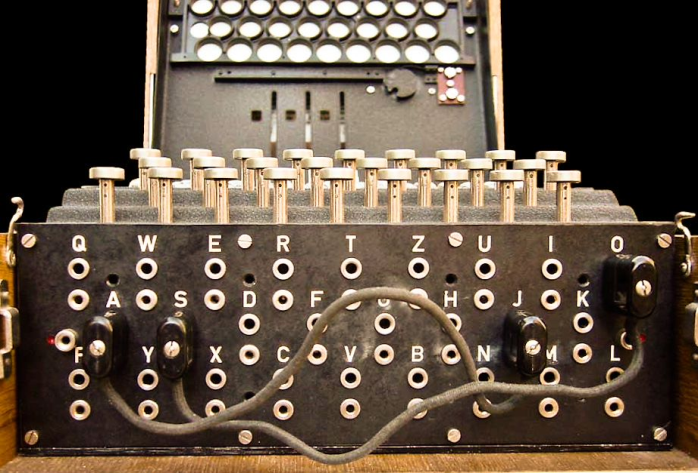
Możemy zaobserwować, że praktycznie pokrywa się to ze statystyką w Sherlocku gdzie ta szansa wynosiła ponad 12%. Może to być tylko przypadek ale, i tak obserwacja warta pokazania.

Uważamy, że nasz program, ma ogromny potencjał. Mamy wiele interesujących pytań, na które poszukujemy odpowiedzi. Zajmujemy się tematem permutacji na tyle krótko, że zdajemy sobie sprawę, że nasz program nie jest jeszcze finalnym produktem. Z drugiej strony zajmujemy się tematem permutacji na tyle długo, że udała nam się prototyp programu napisać ☺. Będziemy nad nim pracować i może coś ciekawego nam wyjdzie w przyszłości. Na płycie CD znajduje się kopia programu. Zachęcamy do jego wypróbowania i analizy własnych tekstów.

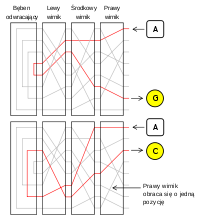
7!/6!

Enigma była maszyną skonstruowaną w 1918r. przez niemieckiego inżyniera Artura Scherbiusa. Po kilku latach została maszyną szyfrującą niemieckiego wojska. Maszyna kodowała na podstawie permutacji poszczególnych liter 26-elementowego alfabetu. System kodujący składał się z trzech wirników, bębna odwracającego (reflektora) oraz łącznicy kablowej. Każdy wirnik posiadał 26 ustawień i każde ustawienie odpowiadało konkretnej literze. Różne kombinacje ich ułożenia tworzą kod, np. AAA lub ABC, lub RMB. Takich kombinacji można było stworzyć około 17000, oznacza to, że przy codziennej zmianie kodu (jak Niemcy robili) można było przez 40 lat nie powtórzyć jednej kombinacji.

Przykładowo po naciśnięciu klawisza z literą J wysłany został sygnał elektryczny. Trafiał on najpierw do łącznicy kablowej pokazanej na zdjęciu:



Łącznica była obsługiwana ręcznie. Prąd trafiał do bananowej wtyczki i przez kabel przemieszczał się do drugiej, dokonując pierwszej permutacji (J,A). Taki system komplikował szyfr tak bardzo, że wymuszał użycie maszyn, a nie metody ręcznej. Następnie sygnał trafia do serca maszyny czyli wirników.



Przed wirnikami sygnał przechodził przez walec wstępny, nie dokonywał on żadnych permutacji, ale zwiększał komplikację okablowania systemu wirników, co utrudniało pracę nad rozszyfrowaniem maszyny. Jak widać na obrazku impuls przemieszcza się przez prawy wirnik, A permutuje na B, po przebyciu kolejnego wirnika pozostaje na B, lewy wirnik to zmiana na D. Teraz bęben odwraca sygnał, który permutuje kolejno na C, F oraz G.

Schemat, co oczywiste, jest uproszczony z 26 liter do 7.

Później prąd wraca przez walec wstępny do łącznicy kablowej, gdzie G podmieniane jest na inną literę, niech to będzie M. Teraz już tylko podświetlana jest lampka z ostateczną literą M. Można powiedzieć, że zaszła permutacja (J,A,B,D,C,F,G,M).

Wróćmy jeszcze do schematu. Jego dolna część przedstawia jak sygnał przebędzie drogę przez wirniki jeżeli ta sama litera zostanie wprowadzona. Po wciśnięciu jakiegokolwiek klawisza, najczęściej prawy wirnik zmienia swoją pozycję o 1 (jeżeli prawy licznik zmienił swoją pozycję określoną ilość razy to zmieniała się pozycja środkowego itd.). Czyli jeżeli mamy do czynienia z kluczem AAA, po naciśnięciu jakiejś litery klucz zmieni się na AAB, przez co jeżeli zapiszemy np. wyraz “MAMA”, to powtarzające się litery M oraz A nie będą zakodowane tak samo jak pierwsze M i A. Enigma posiada mnóstwo utrudnień i haczyków, jest natomiast jedna kwestia, która ułatwia odszyfrowanie. Mowa o bębenku odwracającym, jego własnością było to, że jeżeli do wirników trafi np. litera P, to nigdy po opuszczeniu wirników nie będzie w takiej samej postaci. Wydaje się to mądre i przemyślane, ale przy rozszyfrowywaniu enigmy było wiadome, że zakodowana litera w rzeczywistości nie jest w takiej samej postaci.

W latach 20 i 30 XX wieku zachodnie wywiady próbowały rozszyfrować kod, ale poddali się, uważali, że jest to niemożliwe. Polski wywiad jednak podjął to zadanie. Trzyosobowy zespół stworzyli młodzi matematycy z Poznania: Marian Rejewski, Henryk Zygalski i Jerzy Różycki. Przypadkowo jedna z enigm trafiła w ręce polskiego wywiadu, Polacy więc znali maszynę od wewnątrz, wiedzieli jaką drogę musi pokonać sygnał aby litera została ostatecznie podmieniona.

Pierwszy raz udało się złamać kod w 1932r. Rejewski skorzystał z lenistwa szyfrantów i próbował takich banalnych kluczy jak AAA, ABC czy XYZ. Po odszyfrowaniu kilku depeszy zauważył, że większość z nich zaczyna się od liter “anx”. An z Niemieckiego oznacza “do”, a “x” to znak interpunkcyjny. Polski zespół z przechwyconych wiadomości brał pierwsze trzy litery np. “stn”, które miały znaczyć “anx” i wprowadzali literkę s do czasu kiedy podświetlona została a. Potem naciskali t, jeżeli nie podświetliła się inna litera niż n rozpoczynali proces od nowa. Jeżeli udało im się rozszyfrować znaczenie anx mogli poznać klucz dzienny. Sposób taki był niezawodny, ale czasochłonny, bo maksymalnie trzeba było wcisnąć s 17 576 razy. Kiedy Niemcy zaczęli komplikować zmianę kodów, oraz w enigmach w marynarce wprowadzono 4 wirnik, metoda stała się bezużyteczna. Ponadto zaczęto zamieniać wirniki miejscami, co zwiększyło liczbę możliwych kodów do 105 tysięcy, liczba połączeń na łącznicy kablowej także wzrosła. Trzeba było więc skierować się ku metodom mechanicznym. W 1935r. Rejewski skonstruował cyklometr, posiadał on dwa zestawy wirników enigmy i służył do zapisania wszystkich możliwych kombinacji ułożenia wirników (105 tys). Po roku pracy osiągnięto sukces i odgadnięcie klucza dziennego trwało około 15 minut. Niemcy wciąż jednak udoskonalali enigmę, za nimi podążali Polacy, stworzono bombę kryptologiczną, a po 1939r. dalsze próby złamania szyfrów poprzez udoskonalanie metod Polaków przeniesiono do Anglii, gdzie dzięki zastosowaniu wynalazków trójki z Poznania udało się skrócić przebieg drugiej wojny światowej o kilka lat.

ZAKOŃCZENIE

Permutacji możemy użyć w celu:

- obliczenia wszystkich możliwych ustawień, np. w czteroelementowym kodzie,

- rozwiązania niektórych zadań bądź łamigłówek,

- ułożenia kostki Rubika.

Permutacje odgrywają ważną rolę w różnego rodzaju oprogramowaniach. Używa się ich w informatyce. Za ich pomocą koduje oraz programuje się wiele systemów. W programach komputerowych również posiadają niezbędną rolę. Bez nich byłoby o wiele trudniej w wielu dziedzinach naszego życia. Warto również odnotować, że właśnie dzięki permutacjom, polscy uczeni, podczas wojny światowej zdołali złamać kody niemieckiej maszyny szyfrującej Enigmy. Gdyby nie to, kto wie jak mogłyby potoczyć się dalsze losy wojny.

Pracę tą ciężko było samodzielnie zrobić z powodu małej dostępności wiedzy o permutacjach, ale mamy nadzieję, że Wam się podobało. Zachęcamy Was do zrobienia zadań, na stronach 23 i 24 , które z pewnością pomogą Wam utrwalić świeżo nabyte informacje. Myślimy, że permutacje są naprawdę ciekawe i mają jeszcze wiele innych możliwości. Szczególnie ekscytujące było zaproponowanie swoich propozycji działań, zadań czy pojęć i programu komputerowego. Warto było napisać tą pracę i wiele się o nich nauczyć, choć łatwo nie było.

Dziękujemy za przeczytanie jej. Mamy nadzieję, że sporo się nauczyliście i nie był to dla Was zmarnowany czas !

ZADANIA DO ROZDZIAŁU 1! (odpowiedzi pod zadaniami)

1. Ile jest wszystkich możliwych permutacji na zbiorze 6 – elementowym ?

2. Zapisz dwoma innymi sposobami permutację (3,2,4,1).

3. Zapisz w nawiasie jaka permutacja została napisana strzałkami.

1 4

2 1

3 2

4 3

ZADANIA DO ROZDZIAŁU 2! (odpowiedzi pod zadaniami)

1. Oblicz.

a) (1,3,4) \* (2,4) ,

b) (4,1,5) \* (2,4,5).

2. Oblicz :

a) rząd cyklu ( 2,4,1,6,2,7),

b) rząd permutacji (2,3) \* (2,1,4).

3. Oblicz rząd iloczynu cykli (1,3,5,2,4) \* (1,3,6).

4. Oblicz :

a) =

b) =

5. Oblicz :

a) =

b) =

ZADANIA DO ROZDZIAŁU 3!/2 (odpowiedzi pod zadaniami)

1. Rozwiąż równania :

a) X =

b) X =

ZADANIA DO ROZDZIAŁU 4!/3!

Wykonaj działania

1. (2,4) (1,2,4)
2. (3,4) (1,2,4)
3. (3,5,4,6) (2,5,3)

ZADANIA DO ROZDZIAŁU 5!/24

1. Oblicz liczbę permutacji chaotycznych w zbiorze 6 - elementowym

Odpowiedzi:

1! 1. P6 = 6! = 480 2. , (3,2,4,1), 1 2 3 4 3. ( 1,4,3,2) 2! 4 1 2 3 1. a) (1,3,2,4) b) (1,2,4) 2. a) 6 b) 4 3. 4 4. a) (1,2,3,5,4) b) (1,4) \* (3,6) 5. 1 a) ( 1,3,2,4,5 ) b) (1,6) \* (2,3,5,4) 3!/2 1. a) (1,3,2) b) (1,2,5,4)

4!/3!

1. (1,2) (3,4)
2. (1,2,4,3)
3. (1,3) (2,5,4,6)

5!/24

265

6!-714

* W języku Walijskim IE oznacza tak, natomiast przy EI tłumacz wariuje, pokazując, że albo nic nie znaczy albo, że oznacza: jego, mu, to, tego, jej, stawać się, osiągać, sprzedawać i jeszcze kilka. Całkiem interesujący przypadek.
* W języku greckim natomiast Ναί oznacza tak, a przy ίnα tłumacz pokazuje: błonnik, włókno i struktura.
* Mi się udało znaleźć następujące wyrazy: warty, wryta, trawy.