# Zastosowanie algebry logiki
## do teorji szyfrów.

Napisał

**Edward Stamm.**

---

Pewna klasa szyfrów daje się zdefiniować jako rezultat przekształcenia grup znaków (liter, kombinacji liter, cyfr, liczb i interpunkcji) na inne grupy znaków. Przekształcenie to obraca się w zakresie skończonym. Nic więc naturalniejszego, jak zwrócić się do algebry logiki która z natury rzeczy może być z łatwością dostosowana do zakresów skończonych.

Zajmę się tutaj przykładem przekształcenia pojedynczych liter na litery pojedyncze, czyli pewnego rodzaju szyfrowaniem liter i słów z wykluczeniem cyfr (liczb) i interpunkcji. Zaznaczam przytem, że nie mam na razie na oku praktycznego zastosowania, lecz badam całą sprawę ze stanowiska matematyka. Być może, że z tego względu będą rezultaty badań ze stanowiska praktycznego mało ważne; jednak ze stanowiska teoretycznego przypisuję im pewną wagę.

Naszym zakresem niechaj będą litery

(1) a, ą, b, c, ć, d, e, ę, f, g, h, i, j, k, l, ł, m, n, ń, o, ó, p, r, s (ś), t, u, v, w, x, y, z (ź), ż.

Pragniemy więc przekształcić słowa składające się z tych liter, lub pojedyncze litery z podanego zakresu na inne. Pragniemy je następnie przekształcić zapomocą równań transformacyjnych, opartych na działaniach algebry logiki. Innemi słowy, chcemy uważać zakres podanych liter za zakres logiczny. Nadmieniamy, że litery

wzięte w nawias uważamy za równoważne z literami stojącemi przed nawiasem, więc literę $s$ za równoważną z literą $ś$, literę $z$ za równoważną z literą $ź$.

Aby nasz zakres liter uczynić zakresem logicznym posługujemy się metodą Huntingtona, ogłoszoną w rozprawie „Sets of independent postulates for the Algebra of Logic". [1])

Przedewszystkiem konstatujemy, że nasz zakres może być logicznym, ponieważ zawiera $2^n = 32$ elementy. Po skonstatowaniu tego należy jeszcze określić odpowiednio sumę logiczną, iloczyn logiczny i negację. Stosownie do podanej metody obieramy na zero logiczne np. literę $v$. Następnie wybieramy najmniejsze składniki.[2]) Niechaj będą nimi ze względu, że $n = 5$

$$s_1 = a,\ s_2 = e,\ s_3 = i,\ s_4 = o,\ s_5 = u. \tag{2}$$

Sumy określamy w następujący sposób:

$$\begin{aligned}
&s_1 \cup s_2 = p_{12} = ą \\
&s_1 \cup s_3 = p_{13} = b \\
&s_1 \cup s_4 = p_{14} = c \\
&s_1 \cup s_5 = p_{15} = ć \\
&s_2 \cup s_3 = p_{23} = d \\
&s_2 \cup s_4 = p_{24} = ę \\
&s_2 \cup s_5 = p_{25} = f \\
&s_3 \cup s_4 = p_{34} = g \\
&s_3 \cup s_5 = p_{35} = h \\
&s_4 \cup s_5 = p_{45} = j \\
&s_1 \cup s_2 \cup s_3 = p_{123} = k \\
&s_1 \cup s_2 \cup s_4 = p_{124} = l \\
&s_1 \cup s_2 \cup s_5 = p_{125} = ł \\
&s_1 \cup s_3 \cup s_4 = p_{134} = m \\
&s_1 \cup s_3 \cup s_5 = p_{135} = n \\
&s_1 \cup s_4 \cup s_5 = p_{145} = ń \\
&s_2 \cup s_3 \cup s_4 = p_{234} = ó
\end{aligned} \tag{2a}$$

[1]) Trans. of the Amer. Math. Soc. tom 5, 1904, str. 308 i nast. lub 2) str. 30 n.

[2]) Por. moją Algebrę Logiki, Warszawa 1913, str. 28 n.

$$s_2 \cup s_3 \cup s_5 = p_{235} = p$$
$$s_2 \cup s_4 \cup s_5 = p_{245} = r$$
$$s_3 \cup s_4 \cup s_5 = p_{345} = s(\acute{s})$$
$$s_1 \cup s_2 \cup s_3 \cup s_4 = p_{1234} = t$$
$$s_1 \cup s_2 \cup s_3 \cup s_5 = p_{1235} = w$$
$$s_1 \cup s_2 \cup s_4 \cup s_5 = p_{1245} = y$$
$$s_1 \cup s_3 \cup s_4 \cup s_5 = p_{1345} = z(\acute{z})$$
$$s_2 \cup s_3 \cup s_4 \cup s_5 = p_{2345} = \acute{z}$$
$$s_1 \cup s_2 \cup s_3 \cup s_4 \cup s_5 = p_{12345} = x.$$

Znak $\cup$ jest symbolem sumy logicznej.

Wynika z tego, że na ogół logiczny wybieramy literę $x$. — Ponieważ suma logiczna dwu dowolnych przedmiotów jest wtedy określona wzorem

$$p_{k\ldots m} \cup p_{r\ldots t} = p_{k\ldots mr\ldots t}$$

gdzie $k\ldots mr\ldots t$ zawiera wskaźniki przedmiotu

$$p_{k\ldots m}$$

i przedmiotu

$$p_{r\ldots t}$$

więc tablica sum logicznych przedstawia się w następujący sposób:

| | v | a | ą | b | c | ć | d | e | ę | f | g | h | i | j | k | l | ł | m | n | ń | o | ó | p | r | s | t | u | w | y | z | ż | x |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| v | v | a | ą | b | c | ć | d | e | ę | f | g | h | i | j | k | l | ł | m | n | ń | o | ó | p | r | s | t | u | w | y | z | ż | x |
| a | a | a | ą | b | c | ć | k | ą | l | ł | m | n | b | ń | k | l | ł | m | n | ń | c | t | w | y | z | t | ć | w | y | z | x | x |
| ą | ą | ą | k | l | ł | k | ą | l | ł | t | w | k | y | k | l | ł | t | w | y | l | t | w | y | x | t | ł | w | y | x | x | x |
| b | b | b | k | b | m | n | k | k | t | w | m | n | b | z | k | t | w | m | n | z | m | t | w | x | z | t | n | w | x | z | x | x |
| c | c | c | l | m | c | ń | t | l | l | y | m | z | m | ń | t | l | y | m | z | ń | c | t | x | y | z | t | ń | x | y | z | x | x |
| ć | ć | ć | ł | n | ń | c | w | ł | y | ł | z | n | n | ń | w | y | ł | z | n | ń | ń | x | w | y | z | x | ć | w | y | z | x | x |
| d | d | k | k | k | t | w | d | d | ó | p | ó | p | d | ż | k | t | w | t | w | x | ó | o | p | ż | ż | t | p | w | x | x | ż | x |
| e | e | ą | ą | k | l | ł | d | e | ę | f | ó | p | d | r | k | l | ł | t | w | y | ę | ó | p | r | ż | t | f | w | y | x | ż | x |
| ę | ę | l | l | t | l | y | ó | ę | ę | r | ó | ż | ó | r | t | l | y | t | x | y | ę | o | ż | r | z | t | r | x | y | x | ż | x |
| f | f | ł | ł | w | y | ł | p | f | r | f | ż | p | p | r | w | y | ł | x | w | y | r | ż | p | r | ż | x | f | w | y | x | ż | x |
| g | g | m | t | m | m | z | ó | ó | ó | ż | g | s | g | s | t | t | x | m | z | z | g | ó | ż | ż | s | t | s | x | x | z | ż | x |
| h | h | n | w | n | z | n | p | p | ż | p | s | h | h | s | w | x | w | z | n | z | s | ż | p | ż | s | x | h | w | x | z | ż | x |
| i | i | b | k | b | m | n | d | d | ó | p | g | h | i | s | k | t | w | m | n | z | g | ó | p | ż | s | t | h | w | x | z | ż | x |
| j | j | ń | y | z | ń | ń | ż | r | r | r | s | s | s | j | x | y | y | z | z | ń | j | ż | ż | r | s | x | j | x | y | z | ż | x |
| k | k | k | k | k | t | w | k | k | t | w | t | w | k | x | k | t | w | t | w | x | t | t | w | x | x | t | w | w | x | x | x | x |
| l | l | l | l | t | l | y | t | l | l | y | t | x | t | y | t | l | y | t | x | y | l | t | x | y | x | t | y | x | y | x | x | x |
| ł | ł | ł | ł | w | y | ł | w | ł | y | ł | x | w | w | y | w | y | ł | x | w | y | y | x | w | y | x | x | ł | w | y | x | x | x |
| m | m | m | t | m | m | z | t | t | t | x | m | z | m | z | t | t | x | m | z | z | m | t | x | x | z | t | z | x | x | z | x | x |
| n | n | n | w | n | z | n | w | w | x | w | z | n | n | z | w | x | w | z | n | z | z | x | w | x | z | x | n | w | x | z | x | x |
| ń | ń | ń | y | z | ń | ń | x | y | y | y | z | z | z | ń | x | y | y | z | z | ń | ń | x | x | y | z | x | ń | x | y | z | x | x |
| o | o | c | l | m | c | ń | ó | ę | ę | r | g | s | g | j | t | l | y | m | z | ń | o | ż | z | r | s | t | j | x | y | z | ż | x |
| ó | ó | t | t | t | t | x | ó | ó | ó | ż | ó | ż | ó | ż | t | t | x | t | x | x | ó | ó | ż | ż | ż | t | ż | x | x | x | ż | x |
| p | p | w | w | w | x | w | p | p | ż | p | ż | p | p | ż | w | x | w | x | w | x | ż | ż | p | ż | ż | x | p | w | x | x | ż | w |
| r | r | y | y | x | y | y | z | r | r | r | ż | ż | ż | r | x | y | y | x | x | y | r | ż | ż | r | ż | x | r | x | y | x | ż | x |
| s | s | z | x | z | z | z | i | ż | ż | ż | s | s | s | s | x | x | x | z | z | z | s | ż | ż | ż | s | x | s | x | x | z | ż | x |
| t | t | t | t | t | t | x | t | t | t | x | t | x | t | x | t | t | x | t | x | x | t | t | x | x | x | t | x | x | x | x | x | x |
| u | u | ć | ł | n | ń | ć | p | f | r | f | s | h | h | j | w | y | ł | z | n | ń | j | ż | p | r | s | x | u | w | y | z | ż | x |
| w | w | w | w | w | x | w | w | w | x | w | x | w | w | x | w | x | w | x | w | x | x | x | w | x | x | x | w | w | x | x | x | x |
| y | y | y | y | x | y | y | x | y | y | y | y | x | x | x | y | x | y | y | x | x | y | y | x | x | y | x | x | x | y | x | x | x |
| z | z | z | x | z | z | z | x | x | x | x | z | z | z | z | x | x | x | z | z | z | z | x | x | x | z | x | z | x | x | z | x | x |
| ż | ż | x | x | x | x | x | ż | ż | ż | ż | ż | ż | ż | ż | x | x | x | x | x | x | ż | ż | ż | ż | ż | x | ż | x | x | x | ż | x |
| x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x |

(3)

Iloczyn logiczny określa się wzorem

$$p_K \cap p_L = p_M$$

gdzie znak $\cap$ jest symbolem iloczynu logicznego, a $M$ zawiera wskaźniki wspólne przedmiotów $p_K$ i $p_L$. Jeżeli więc np.

$$p_K = p_{245} = r \qquad \text{a} \qquad p_L = p_{1235} = w$$

to wtedy mamy

$$p_K \cap p_L = p_{245} \cap p_{1235} = p_{25} = f.$$

Tablica iloczynów logicznych przedstawia się więc w następujący sposób:

(4)

| | v | a | ą | b | c | ć | d | e | ę | f | g | h | i | j | k | l | ł | m | n | ń | o | ó | p | r | s | t | u | w | y | z | ż | x |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v |
| a | v | a | a | a | a | a | v | v | v | v | v | v | v | a | a | a | a | a | a | a | v | v | v | v | a | v | a | a | a | v | a | |
| ą | v | a | ą | a | a | a | e | e | e | e | v | v | v | v | ą | ą | ą | a | a | a | v | e | e | e | v | ą | v | ą | ą | a | e | ą |
| b | v | a | a | b | a | a | i | v | v | v | i | i | i | v | b | a | a | b | b | a | v | i | i | v | i | b | v | b | a | b | i | b |
| c | v | a | a | a | c | a | v | v | o | v | o | v | v | o | a | c | a | c | a | c | o | o | v | o | o | c | v | a | c | c | o | c |
| ć | v | a | a | a | a | ć | v | v | v | u | v | u | v | u | a | a | ć | a | ć | ć | v | v | u | u | u | a | u | ć | ć | ć | u | ć |
| d | v | v | e | i | v | v | d | e | e | e | i | i | i | v | d | e | e | i | i | v | v | d | d | e | i | d | v | d | e | i | d | d |
| e | v | v | e | v | v | v | e | e | e | e | v | v | v | v | e | e | e | v | v | v | v | e | e | e | v | e | v | e | e | v | e | e |
| ę | v | v | e | v | o | v | e | e | ę | e | o | v | v | o | e | ę | e | o | v | o | o | ę | e | ę | o | ę | v | e | ę | o | ę | ę |
| f | v | v | e | v | v | u | e | e | e | f | v | u | v | u | e | e | f | v | u | u | v | e | f | f | u | e | u | f | f | u | f | f |
| g | v | v | v | i | o | v | i | v | o | v | g | i | i | o | i | o | v | g | i | o | o | g | i | o | g | g | v | i | o | g | g | g |
| h | v | v | v | i | v | u | i | v | v | u | i | h | i | u | i | v | u | i | h | u | v | i | h | u | h | i | u | h | u | h | h | h |
| i | v | v | v | i | v | v | i | v | v | i | i | i | v | i | v | v | i | i | v | v | i | i | v | v | i | i | v | i | v | i | i | i |
| j | v | v | v | v | o | u | v | v | o | u | o | u | v | j | v | o | u | o | u | j | o | o | u | j | j | j | o | u | u | j | j | j |
| k | v | a | a | b | a | a | d | e | e | e | i | i | i | v | k | a | a | b | b | a | v | d | d | e | i | k | v | k | a | b | d | k |
| l | v | a | a | a | c | a | e | e | e | e | e | o | v | v | o | ą | l | ą | c | a | c | o | e | e | e | o | l | v | a | l | c | e | l |
| ł | v | a | ą | a | a | ć | e | e | e | f | v | u | v | u | a | ą | ł | a | ć | ć | v | e | f | f | u | a | u | ł | ł | ć | f | t |
| m | v | a | a | b | c | a | i | v | o | v | g | i | i | o | b | c | a | m | b | c | o | g | i | o | g | m | v | b | c | m | g | m |
| n | v | a | a | b | a | ć | i | v | v | u | i | h | i | u | b | a | ć | b | n | ć | v | i | h | u | h | b | u | n | ć | n | h | n |
| ń | v | a | a | a | c | ć | v | v | o | u | o | u | v | j | a | c | ć | c | ć | ń | o | o | u | j | j | c | u | ć | ń | ń | j | ń |
| o | v | v | v | v | o | v | v | v | o | v | o | v | o | v | o | v | o | v | o | v | o | o | o | v | o | o | o | v | v | o | o | o |
| ó | v | v | e | i | o | v | d | e | ę | e | g | i | i | o | d | e | e | g | i | o | o | ó | t | e | g | ó | v | d | e | g | ó | ó |
| p | v | v | e | i | v | u | d | e | e | f | i | h | i | u | d | e | f | i | h | u | v | d | p | f | h | d | u | p | f | h | p | p |
| r | v | v | e | v | o | u | e | e | ę | f | o | u | v | j | e | ę | f | o | u | j | o | ę | f | r | j | ę | u | f | r | j | r | r |
| s | v | v | v | i | o | u | i | v | o | u | g | h | i | j | i | o | u | g | h | j | o | g | h | j | s | g | u | h | j | s | s | s |
| t | v | a | ą | b | c | a | d | e | ę | e | g | i | i | o | k | l | ą | m | b | c | o | ó | d | ę | g | t | v | k | l | m | ó | t |
| u | v | v | v | v | u | v | v | v | u | v | u | v | u | v | v | u | v | u | u | v | v | u | u | u | v | u | u | u | u | u | u | u |
| w | v | a | ą | b | a | ć | d | e | e | f | i | h | i | u | k | ą | ł | b | n | ć | v | d | p | f | h | k | u | w | ł | n | p | w |
| y | v | a | ą | a | c | ć | e | e | ę | f | o | u | v | j | ą | l | ł | c | ć | ń | o | ę | f | r | j | l | u | ł | y | ń | r | y |
| z | v | a | a | b | c | ć | i | v | o | u | g | h | i | j | b | c | ć | m | n | ń | o | g | h | j | s | m | u | n | ń | z | s | z |
| ż | v | v | e | i | o | u | d | e | ę | f | g | h | i | j | d | e | f | g | h | j | a | ó | p | r | s | ó | u | p | r | s | ż | ż |
| x | v | a | ą | b | c | ć | d | e | ę | f | g | h | i | j | k | l | ł | m | n | ń | o | ó | p | r | s | t | u | w | y | z | ż | x |

Negacja logiczna określa się wzorem

$$(p_K)' = p_{K'}$$

gdzie symbol $'$ oznacza negację, a $k'$ zawiera wszystkie cyfry nie należące do $K$. Mamy więc np.

$$(p_{135})' = p_{14} = (p)' = c.$$

Tablica negacji logicznych ma więc postać:

$$\begin{array}{c} \text{v a ą b c ć d e ę f g h i j k l ł m n ń o ó p r s t u w y z ż x} \\ \hline \text{x ż s r p ó ń z n m ł l y k j h g f ę d w ć c b ą u t o i e a v} \end{array} \qquad (5)$$

Po tem określeniu sumy logicznej, iloczynu logicznego i negacji możemy zastosować do naszego zakresu liter wszystkie twierdzenia algebry logiki.

Jeżeli chodzi nam o zaszyfrowanie tekstu, składającego się z naszego zakresu liter, będziemy mogli oprzeć się na funkcji logicznej

$$y = a\,x \cup b\,x' \qquad (6)$$

gdzie $a\,x$ oznacza iloczyn logiczny liter $a$ i $x$, zaś $b\,x'$ iloczyn logiczny liter $b$ i negacji $x$. Wstawiając wtedy za $a$ i $b$ stałe lub zmienne litery, zresztą dowolne, — będziemy litery te nazywali w s k a ź n i k i e m — zaś za $x$ litery, które mamy zaszyfrować, czyli jak się będziemy wyrażali s z y f r a n t y, otrzymamy wykonując na podstawie podanych wyżej tablic wskazane działanie logiczne. litery zaszyfrowane, czyli jak będziemy mówili s z y f r a t y.

Przykład: Niechaj będzie

$$a = 1, \quad b = m, \quad x = s.$$

Mamy wtedy

$$a\,x = ls = o, \quad x' = s' = ą, \quad b\,x' = m\,ą = a, \quad a\,x \cup b\,x' = o \cup a = c.$$

Przy wskaźniku $l, m$ jest więc szyfratem litery $s$.

Jeśli chcemy dany szyfrat odszyfrować z powrotem należy oczywiście równania transformacyjne (6) rozwiązać względem $x$. Po rozwiązaniu otrzymamy

$$x = (a\,y \cup a'\,y')\,u \cup (b'\,y \cup b\,y')\,u',$$

gdzie $u$ jest dowolnym parametrem. Wynika z tego, że $x$ jest wieloznaczne. Aby $x$ było jednoznaczne, musi być

$$a\,y \cup a'\,y' = b'\,y \cup b\,y'.$$

Daje to

$$a = b'.$$

Równanie (6) otrzymuje wtedy postać

$$y = b'x \cup bx',$$

czyli, jeżeli zamiast $b$ napiszemy $p$,

$$y = p'x \cup px'. \tag{7}$$

Ponieważ warunek jednoznaczności dla funkcji jest konieczny do odszyfrowania, a funkcja (7) jest pierwotniakiem, możemy powiedzieć, że o ile chodzi o wskaźnik o jednym zmiennym (lub stałym) parametrze, musi równanie transformacyjne przy szyfrowaniu i odszyfrowywaniu mieć postać równania (7), czyli odpowiednia funkcja musi być pierwotniakiem (pierwotkiem) 1-go stopnia. [1])

W tym wypadku więc odbywa się szyfrowanie w naszym zakresie (1), oraz odszyfrowywanie na podstawie równań transformacyjnych

$$\begin{aligned} y &= p'x \cup px' \\ x &= p'y \cup py'. \end{aligned} \tag{8}$$

Weźmy teraz pod uwagę spółczynnik (wskaźnik) $p$. Jeżeli będzie on stały, wtedy każda litera $x$ będzie przedstawiona zawsze przez tę samą literę $y$ szyfratu. Jest to oczywiście bardzo wielkie ułatwienie przy odszyfrowywaniu przez strony niepowołane. Odszyfrowywanie należy w tym wypadku do najłatwiejszych.

Możemy jednak założyć, że $p$ jest zmienne. W tym wypadku wybieramy dla $p$ pewien skończony, uporządkowany zakres, np.

$$p = (p_i, p_k, \ldots\ldots, p_n), \tag{9}$$

w którym następstwo liter $p_i$, $p_k$,..... zostaje niezmienione. Wtedy wstawiamy przy kolejnem szyfrowaniu liter za $p$ kolejno litery $p_i$. $p_k$,..... $p_n$, a potem z powrotem $p_i$. $p_k$,... i t. d. W tym wypadku jest tasama litera $x$ przedstawiona w szyfracie przez różne litery, co utrudnia niepowołane odszyfrowanie.

Przykład: Mamy zaszyfrowac tekst: „teorya szyfrów“. Wskaźnikiem niechaj będzie grupa liter

radio.

---

[1]) l. c. str. 74 n.

Otrzymujemy:

$$y = p'x \cup px' = r't \cup rt' = bt \cup ru = b \cup u = n$$
$$= a'e \cup ae' = że \cup az = e \cup a = ą$$
$$= d'o \cup do' = ńo \cup dw = o \cup d = ó$$
$$= i'r \cup i_1'r' = yr \cup ib = r \cup i = ż$$
$$= o'y \cup oy' = wy \cup oi = ł \cup v = ł$$
$$= r'a \cup ra' = ba \cup rż = a \cup r = y$$
$$= a's \cup as' = żs \cup aą = s \cup a = z$$
$$= d'z \cup dz' = ńz \cup de = ń \cup e = y$$
$$= i'y \cup iy' = yy \cup ii = y \cup i = x$$
$$= c'f \cup cf' = wf \cup om = f \cup o = r$$
$$= r'r \cup rr' = br \cup rb = v \cup v = v$$
$$= a'ó \cup aó' = żó \cup ać = ó \cup a = t$$
$$= d'w \cup dw' = ńw \cup do = ć \cup v = ć.$$

Szyfratem tekstu „teorja szyfrów“ przy wskaźniku „radio“ jest grupa liter

nąćżłyzyxrvtć.

W praktyce dzieli się zazwyczaj szyfrat na stałe grupy liter np. po 5. Ponieważ nam chodzi tylko wyłącznie o rezultaty teoretyczne, więc uważamy podział ten za zbyteczny.

Przy zmiennym wskaźniku przedstawia równanie transformacyjne

$$y = p'x \cup px'$$

funkcję logiczną o dwu zmiennych $p, x$:

$$y = f(p, x).$$

Dla ułatwienia szyfrowania możemy bardzo łatwo, korzystając z tej uwagi sporządzić na miejsce tablic iloczynów, sum i negacji jedną jedyną tablicę, która poda nam wprost dla każdego $p$ i $x$ odpowiednią wartość dla $y$. Piszemy w pierwszym wierszu wszystkie możliwe wartości $x$, w pierwszej kolumnie wszystkie możliwe wartości $p$, a w odpowiednich kratkach odpowiednie wartości dla $y$, według równania (7).

| | v | a | ą | b | c | ć | d | e | ę | f | g | h | i | j | k | l | ł | m | n | ń | o | ó | p | r | s | t | u | w | y | z | ż | x |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| v | v | a | ą | b | c | ć | d | e | ę | f | g | h | i | j | k | l | ł | m | n | ń | o | ó | p | r | s | t | u | w | y | z | ż | x |
| a | a | v | e | i | o | u | k | ą | l | ł | m | n | b | ń | d | e | f | g | h | j | c | t | w | y | z | ć | c | p | r | s | x | ż |
| ą | ą | e | v | d | ę | f | b | a | c | c | t | w | k | y | i | o | u | ó | p | r | l | m | n | ń | x | g | ł | h | j | ż | z | s |
| b | b | i | d | v | g | h | ą | k | t | w | c | ć | a | z | e | ó | p | o | u | s | m | l | ł | x | ń | ę | n | f | ż | j | y | r |
| c | c | o | ę | g | v | j | t | l | ą | y | b | z | m | ć | ó | e | r | i | s | u | a | k | x | ł | n | d | ń | ż | f | h | w | p |
| ć | ć | u | f | h | j | v | w | ł | y | ą | z | b | n | c | p | r | e | s | i | o | ń | x | k | l | m | ż | a | d | ę | g | t | ó |
| d | d | k | b | ą | t | w | v | i | g | h | ę | f | e | ż | a | m | n | l | ł | x | ó | o | u | s | r | c | p | ć | z | y | j | ń |
| e | e | ą | a | k | l | ł | i | v | o | u | ó | p | d | r | b | c | ć | t | w | y | ę | g | h | j | ż | m | f | n | ń | x | s | z |
| ę | ę | l | c | t | ą | y | g | o | v | j | d | ż | ó | f | m | a | ń | k | x | ł | e | i | s | u | p | b | r | z | ć | w | h | n |
| f | f | ł | c | w | y | ą | h | u | j | v | ż | d | p | ę | n | ń | a | x | k | l | r | s | i | o | ó | z | e | b | c | t | g | m |
| g | g | m | t | c | b | z | ę | ó | d | ż | v | j | o | h | l | k | x | a | ń | n | i | e | r | p | u | ą | s | y | w | ć | f | ł |
| h | h | n | w | ć | z | b | f | p | i | d | j | v | u | g | ł | x | k | ń | a | m | s | r | e | ż | o | y | i | ą | t | c | ę | l |
| i | i | b | k | a | m | n | e | d | ó | p | o | u | v | s | ą | t | w | c | ć | z | g | ę | f | ż | j | l | h | ł | x | ń | r | y |
| j | j | ń | y | z | ć | c | ż | r | f | ę | h | g | s | v | x | ł | l | n | m | a | u | p | ó | e | i | w | o | t | ą | b | d | k |
| k | k | d | i | e | ó | p | a | b | m | n | l | ł | ą | x | v | g | h | ę | f | ż | t | c | ć | z | y | c | w | u | s | r | ń | j |
| l | l | e | o | ć | e | r | m | c | a | ń | k | x | t | ł | g | v | j | d | ż | f | ą | b | ń | ć | w | i | y | s | u | p | n | h |
| ł | ł | f | u | p | r | e | n | ć | ń | a | x | k | w | l | h | j | v | ż | d | ę | y | ń | b | c | t | s | ą | i | o | o | m | g |
| m | m | g | ó | o | i | s | l | t | k | x | a | ń | c | n | ę | d | ż | v | j | h | b | ą | y | w | ć | e | z | r | p | u | ł | f |
| n | n | h | p | u | s | i | ł | w | x | k | ń | a | ć | m | f | ż | d | j | v | g | z | y | ą | t | c | r | b | e | ó | o | l | ę |
| ń | ń | j | r | s | u | o | x | y | ł | l | n | m | z | a | ż | f | ę | h | g | v | ć | w | t | ą | b | p | c | ó | e | i | k | d |
| o | o | c | l | m | a | ń | ó | ę | e | r | i | s | g | u | t | ą | y | b | z | ć | v | d | ż | f | h | k | j | x | ł | n | p | w |
| ó | ó | t | m | l | k | x | o | g | i | s | e | r | e | p | c | b | ń | ą | y | w | d | v | j | h | f | a | z | ń | n | ł | u | ć |
| p | p | w | n | ł | x | k | u | h | s | i | r | e | f | ó | ć | ń | b | y | ą | t | ż | j | v | g | ę | ń | d | a | m | l | o | c |
| r | r | y | ń | x | ł | l | s | j | u | ó | p | ż | ż | e | z | ć | c | w | t | ą | f | h | g | v | d | n | ę | m | a | k | i | b |
| s | s | z | x | ń | n | m | r | ż | p | ó | u | o | j | i | y | w | t | ć | c | b | h | f | ę | d | v | ł | g | l | k | a | ę | ą |
| t | t | ó | g | ę | d | ż | c | m | b | z | ą | y | l | w | o | i | s | e | r | p | k | a | ń | n | ł | v | x | j | h | f | ć | u |
| u | u | c | ł | n | ń | a | p | f | r | e | s | i | h | o | w | y | ą | z | b | c | j | ż | d | ę | g | x | v | k | l | m | ó | t |
| w | w | p | h | f | ż | d | ć | n | z | b | y | ą | ł | t | u | s | i | r | e | ó | x | ń | a | m | l | j | k | v | g | ę | c | o |
| y | y | r | j | ż | f | ę | z | ń | ć | c | w | t | x | ą | s | u | o | p | ó | o | ł | n | m | a | k | h | l | g | v | d | b | i |
| z | z | s | ż | j | h | g | y | x | w | t | ć | c | ń | b | r | p | ó | u | o | i | n | ł | l | k | a | f | m | ę | d | v | ą | e |
| ż | ż | x | z | y | w | t | j | s | h | g | f | ę | r | d | ń | n | m | ł | l | k | p | u | o | i | e | ć | ó | c | b | ą | v | a |
| x | x | ż | s | r | p | ó | ń | z | n | m | ł | l | y | k | j | h | g | f | ę | d | w | ć | c | b | ą | u | t | o | i | e | a | v |

Ponieważ równanie zapomocą którego szyfrujemy jest identyczne z równaniem zapomocą którego odszyfrowujemy (por. równanie 8), więc powyższa tablica służy zarazem i do odszyfrowywania w przyjętych warunkach.

Ponieważ wszystkie prawa algebry logiki stosują się do naszego zakresu (1), a więc do naszej teorji szyfrów, możemy z łatwością interpretować twierdzenia algebry logiki w dziedzinie szyfrów, o ile posiadają one tam jakiś sens. Ograniczamy się przedewszystkiem do problemu następującego.

Wiadomo, że w algebrze logiki daje się każdy przedmiot przedstawić w jeden jedyny sposób przez najmniejsze (ewentualnie największe) składniki.[1]) Znaczy to, że każda litera da się przedstawić w jeden jedyny sposób przez pewną ilość liter specjalnych, a mianowicie w naszym wypadku przez litery szeregu (2), w postaci sumy logicznej (jeżeli chodzi o składniki najmniejsze). Możemy łatwo skonstruować następującą tablicę na podstawie relacji (2a)):

$$a = a$$
$$ą = a \cup e$$
$$b = a \cup i$$
$$c = a \cup o$$
$$ć = a \cup u$$
$$d = e \cup i$$
$$e = e$$
$$ę = e \cup o$$
$$f = e \cup u$$
$$g = i \cup o$$
$$h = i \cup u$$
$$i = i$$
$$j = o \cup u$$
$$k = a \cup e \cup i$$
$$l = a \cup e \cup o$$
$$ł = a \cup e \cup u$$
$$m = a \cup i \cup o$$
$$n = a \cup i \cup u$$
$$ń = a \cup o \cup u$$
$$o = o$$
$$ó = e \cup i \cup o$$

[1]) cf. 2).

(11)
$$p = e \cup i \cup u$$
$$r = e \cup o \cup u$$
$$s = i \cup o \cup u$$
$$t = a \cup e \cup i \cup o$$
$$u = u$$
$$w = a \cup e \cup i \cup u$$
$$y = a \cup e \cup o \cup u$$
$$z = a \cup i \cup o \cup u$$
$$ż = e \cup i \cup o \cup u$$
$$x = a \cup e \cup i \cup o \cup u.$$

Według tych relacji rozłożony tekst, np. „stacya radiotelegraficzna“ przedstawiałby się więc w następujący sposób:

stacya radiotelegraficzna

icu aeio a ao aeou a eou a ei i o aeio e aeo e io eou a eu i ao aiou aiu a.

Oczywiście, że tak zaszyfrowany tekst byłby bardzo łatwy do odszyfrowania. Każda litera $x$ jest tutaj przedstawiona zawsze przez jedną i tę samą grupę. Można jednak metodę tę skombinować z poprzednio przedstawioną, czyli zaszyfrować po rozłożeniu na składniki najmniejsze ostatni szyfrat. Jeżeli chcę np. przytoczony tekst zaszyfrować zapomocą wskaźnika „radio“ posługuję się tabliczką

(12)

| | a | e | i | o | u |
|---|---|---|---|---|---|
| r | y | j | ż | f | ę |
| a | v | ą | b | c | c |
| d | k | i | e | ó | p |
| i | b | d | v | g | h |
| o | c | ę | g | v | j |

Otrzymamy wtedy:

s t ac y ar adio t el eg r af i c z n a iou aeio a ao aeou a eou a ei i o aeio e aeo e io eou a eu i ao aiou aiu a rad iora d io radi o rad i or a d iora d ior a di ora d io r ad iora dio r żcp bęic k bv yąćh c jcp b ęż b ó bężc ż bęf ą eg ęfc k dj ż vó bgfc kvj y.

Tekst „stacya radiotelegraficzna“ wyraża się więc wtedy szyfratem

żcp bęic k bv yąćh c jcp b ęż b ć bężc i bęf ą eg ęfc k dj ż vó bgfc kvj y.

Oczywiście, że taki sposób szyfrowania nie jest ze względów praktycznych ekonomicznym: 24 liter przedstawiamy w szyfracie przez 51. Aby zyskać na ekonomji, możemy posłużyć się następującą metodą: żądamy, aby tekst szyfratu składał się z pewnych ściśle określonych liter, a mianowicie takich, które zawierają jak najmniej elementów Morsego. (Znaczy to, że wykluczamy np. szyfrowanie przez aparat Hughesa, względnie wysuwamy na pierwszy plan szyfrowanie drogą radiotelegraficzną i aparatem Morsego). — W ten sposób możemy w części uzyskać z powrotem tę ekonomię, którą tracimy przez rozkład na wybrane litery. Ponieważ chodzi nam stosownie do tabliczki (12) dla naszego przykładu o pięć liter, które rozlokujemy wewnątrz tabliczki analogicznej do (12) tak, aby w tym samym wierszu nie powtarzała się ta sama litera, ale zresztą dowolnie (w przeciwnym wypadku nie byłoby odszyfrowanie jednoznaczne), wybieramy na ostateczne litery szyfratu tylko litery składające się najwyżej z 2 elementów Morsego, z kropki i kreski:

$$e \cdot \; t - \; i \; .. \; a \; . - \; n \; -. \qquad (13)$$

Na tej podstawie otrzymamy w miejsce tabliczki (12) tabliczkę

| | a | e | i | o | u |
|---|---|---|---|---|---|
| r | i | t | a | n | e |
| a | n | i | a | e | t |
| d | e | i | t | a | n |
| i | n | a | t | i | e |
| o | a | n | i | t | e |

(14)

odnoszącą się oczywiście do wskaźnika „radio“. Szyfrując dawny tekst „stacja radiotelegraficzna“ w ostatni sposób otrzymamy teraz:

s t a c y a r a d i o t e l e g r a f i c z n a

iou aeio a ao aeou a eou a ei i o aeio e aeo e io ecu a eu i ao aiou aiu a rad iora d io radi o rad i or a d iora d ior a di ora d io r ad iora dio r aen nnae e nt iiae a ten n na a a nnae i nnn i ti nnt e ae a na nint ete i

jeżeli teraz zliczymy elementy Morsego w szyfrancie i szyfracie według ostatniej metody, otrzymamy dla szyfrantu 62 elementy, dla szyfratu 86 elementów, czyli na 100 szyfrantu, 139 szyfratu mimo, że litery są przedstawione przeciętnie przez 2·5 liter.

Zapytajmy się teraz, czy nie można w pewnych warunkach przedstawić całego szyfratu przez jedną i tę samą literę.

Nasze ogólne równanie transformacyjne ma postać

$$y = p'x \cup px'. \tag{7}$$

Jeżeli litery szyfratu mają być wszystkie jednakowe, będzie

$$y = c.$$

Daje to równanie

$$c = p'x \cup px'. \tag{15}$$

$x$ jest dowolne, względnie zależne tylko od szyfrantu. Zatem musi być $p$ funkcją logiczną zmiennych $x$ i $c$, względnie zmiennej $x$ i stałej $c$. Rozwiązując równanie (15) względem $p$ otrzymujemy ostatecznie po redukcji

$$p = c'x \cup cx'.$$

Znaczy to, że dla każdego $x = x_0$, czyli jednakich $x$ otrzymamy i jednakie $p$.

Innemi słowy: Szyfrowanie tego rodzaju jest możliwe. Szyfrat składa się wtedy zawsze z jednej i tej samej litery, natomiast jest wskaźnik zbiorem liter naogół różnych i posiada tę własność, że każdej literze $x_0$ szyfrantu odpowiada litera $p_0$ wskaźnika i to stale, że więc właściwie te same litery są przedstawione przez inne stałe, jeżeli za szyfrat będziemy uważali wskaźnik, co ze względów praktycznych (odszyfrowania) jest możliwem.

Przykład.

Szyfrant: s t a c y a r a d i o t e l e g r a f i c z n a
Wskaźnik: v ł z n k z d z r j h ł ż w ż u d z ó j n a c z
Szyfrat: s s s s s s s s s s s s s s s s s s s s s s s s s s

jeżeli na stałą literę szyfratu wybierzemy literę $s$.

Szyfrowanie odbywa się łatwo zapomocą naszej tablicy (10).

Kończę na tem ogólnem naszkicowaniu problemu, w nadziei, że dalsze badania wykażą i praktyczną korzyść rozwiniętej tutaj w najogólniejszych zarysach teorji.

---