KÓDOVÁNÍ A DEKÓDOVÁNÍ ZALOŽENÉ NA MATICÍCH ZOBECNĚNÝCH FIBONACCIHO ČÍSEL

Ivana Matoušová

Abstrakt

V příspěvku bude blíže představeno téma disertační práce a návrh struktury této práce. Příspěvek prezentuje výsledky literární rešerše, představuje významné odborné články, které se zabývají kódováním a dekódováním pomocí zobecněných Fibonacciho čísel a důležitými vlastnostmi těchto čísel. Mezi významné autory těchto článků patří například A. Stakhov, R. Rozin, E. Kilic nebo M. Basu a B. Prasad. Nakonec budou v příspěvku uvedeny směry, kterými by se chtěla doktorandka ve svém výzkumu dále vydat.

Klíčová slova

Fibonacciho čísla, zlatý řez, kódování

1 Představení tématu

1.1 Fibonacciho čísla

Italský matematik Leonardo Pisano (známý rovněž jako Fibonacci) představil ve 13. století posloupnost čísel:

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$

Tuto posloupnost získal, když se snažil popsat rozmnožování králíků za daných podmínek: Předpokládejme, že máme jeden pár králíků 1. ledna. Tomuto páru se narodí další pár 1. února a dále vždy první den každého následujícího měsíce. Nově narozené páry jsou produktivní od druhého měsíce svého života. Králíci neumírají. Výše uvedená posloupnost vyjadřuje počet párů králíků po n měsících. Posloupnost se nazývá Fibonacciho posloupnost a je dána rekurentním vztahem:

$F(n) = F(n-1) + F(n-2)$,

s počátečními podmínkami $F(0) = 0, F(1) = 1$.

Giovanni Domenico Cassini (1625-1712) popsal vztah mezi třemi sousedícími Fibonacciho čísly. Tento vztah je znám jako Cassiniho vzorec:

$F^2(n) - F(n-1)F(n+1) = (-1)^{n+1}$

V 19. století francouzský matematik Francois Edouard Anatole Lucas popsal posloupnost čísel: $2, 1, 3, 4, 7, 11, 18, 29, 47, \ldots$

Posloupnost se nazývá Lucasova posloupnost a je dána stejným rekurentním vztahem:

$L(n) = L(n-1) + L(n-2)$,

avšak s jinými počátečními podmínkami $L(0) = 2, L(1) = 1$.

Další známý francouzský matematik Jacques Philippe Marie Binet v 19. století spojil zlatý řez s Fibonacciho a Lucasovými čísly. Jejich souvislost je vyjádřena Binetovým vzorcem:

$F(n) = \frac{\tau^n - \tau^{-n}(-1)^n}{\sqrt{5}}$,

$L(n) = \tau^n - \tau^{-n}(-1)^n$,

kde $\tau = \frac{1+\sqrt{5}}{2} \approx 1{,}618$.

Rovněž je známo, že $\lim_{n\to\infty} \frac{F(n)}{F(n-1)} = \lim_{n\to\infty} \frac{L(n)}{L(n-1)} = \tau$.

1.2 *Q*-matice

Americký matematik Verner Email Hoggat zavedl [1] *Q*-matici: $Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ a dokázal, že platí následující vztah pro její n-tou mocninu:

$Q^n = \begin{pmatrix} F(n+1) & F(n) \\ F(n) & F(n-1) \end{pmatrix}$,

$det\ Q^n = (-1)^n$.

O této matici se však zmiňuje již Joel Brennner v abstraktu konference konané v roce 1951 [2].

2 Literární rešerše

2.1 Zobecněná Fibonacciho čísla

V roce 1977 [3] Alexey Petrovich Stakhov zavedl tzv. Fibonacciho *p*-čísla:

$F_p(n) = F_p(n-1) + F_p(n-p-1)$, kde $n > p+1; p = 0, 1, 2, \ldots$

s počátečními podmínkami $F_p(1) = F_p(2) = \cdots F_p(p) = F_p(p+1) = 1$.

Takto definovaná posloupnost čísel nám může opět popsat rozmnožování králíků, pokud nově narozené páry dospívají *p* měsíců (u Fibonacciho posloupnosti dospívají jeden měsíc). Tato analogie je blíže popsána v [4], kde autor dále ukazuje, jak můžeme členy této posloupnosti získat sečtením členů Pascalova trojúhelníka, pokud jeho sloupce posuneme vhodným způsobem. Rovněž autor zavádí pojem zlatý *p*-řez („*golden p-ratio*“).

V [5] Stakhov zavádí Q_p-matici, popisuje její vlastnosti, hodnotu determinantu, jak sestavit její inverzní matici a vztah pro její *n*-tou mocninu. Emrah Kilic v [6] zobecnil Binetův vzorec pro Fibonacciho *p*-čísla, dokázal, že jejich charakteristická rovnice nemá násobné kořeny a ukázal, že tato čísla můžeme získat jako součet určitých kombinačních čísel. Další vlastnosti Fibonacciho *p*-čísel jsou popsány například v [7]. E. Kocer, N. Tuglu a A. Stakhov zavedli v [8] další zobecnění Fibonacciho čísel, tzv. *m*-rozšíření Fibonacciho *p*-čísel:

$F_{p,m}(n) = mF_{p,m}(n-1) + F_{p,m}(n-p-1)$, kde $p = 0, 1, 2, \ldots$,

s počátečními podmínkami $F_{pm}(1) = a_1$, $F_{p,m}(2) = a_2, \dots, F_{p,m}(p+1) = a_{p+1}$, kde a_i jsou celá, reálná nebo komplexní čísla. Jejich práce navazuje na [9], [10], [11], [12], [13] a [14], kde jsou zavedena Fibonacciho čísla řádu m:

$F_m(n) = mF_m(n-1) + F_m(n-2); \quad F_m(0) = 0, \quad F_m(1) = 1, \quad m \in \mathbb{R}^+$. Největší zobecnění Fibonacciho čísel popisuje E. Kocer, N. Tuglu a A. Stakhov v [15].

2.2 Kódování založené na maticích zobecněných Fibonacciho čísel

V roce 2006 byl publikován článek [16], ve kterém Stakhov kromě jiného popisuje princip kódování a dekódování založené na Q_p-matici, tedy na zobecněných Fibonacciho čísel, viz Tabulka 1. Díky tomu, že známe hodnotu determinantu kódové matice ${Q_p}^n$, $det{Q_p}^n = (-1)^{pn}$, jsme schopni určit, jaký determinant má mít přijatá matice $E: |detE| = detM$, kde M je původní matice, kterou chceme zakódovat (zpráva, kterou chceme utajit). V přenosovém kanálu posíláme prvky matice M a rovněž hodnotu jejího determinantu. Tato hodnota determinantu nám slouží jako kontrolní prvek. Na mocnině n se předem dohodne odesílatel a příjemce zprávy. V citovaném článku je dále popsána korekční schopnost této metody a je spočítáno, že korekční schopnost metody je v nejjednodušším případě (tj. $p = 1$) rovna 93,33%.

Tabulka 1. Fibonacciho kódování a dekódování

Kódování	**Dekódování**
$M \times {Q_p}^n = E$	$E \times {Q_p}^{-n} = M$

Přínosy této metody popisuje autor rovněž v [17].

Na myšlenku Stakhova navázal B. Prasad a M. Basu, kteří jako kódové matice využívali matice tvořené jinými zobecněními Fibonacciho čísel, [18], [19], [20], [21].

3 Struktura obsahu disertační práce

Disertační práce by měla obsahovat kapitoly:

1. Historie kódování – způsoby kódování a šifrování používané v minulosti.
2. Představení důležitých pojmů, vět, vztahů – Fibonacciho čísla, zlatý řez, zobecněná Fibonacciho čísla
3. Přehled literatury
4. Typy kódování – základní typy a jejich princip
5. Obecný princip Fibonacciho kódování
6. Nalezení nové, vhodné matice ke kódování, jejímiž prvky budou zobecněná Fibonacciho čísla. Tato matice by měla mít snadný obecný předpis pro její determinant, aby tento determinant sloužil jako kontrolní prvek (analogicky jako v [16]). Chceme, aby tato matice byla tvořena zobecněnými Fibonacciho čísly, danými například rekurentním vztahem ${F^*}_p(n) = {F^*}_p(n-2) + {F^*}_p(n-p)$. Dále je potřeba určit obecný předpis pro inverzní matici kódové matice, která má sloužit k dekódování.

Literatura

[1] HOGGAT, Verner Email. *Fibonacci and Lucas numbers*. Palo Alto (CA): Houghton-Mifflin, 1969.

[2] BRENNER, Joel. Lucas´matrix. *The American Mathematical Monthly.* 1951, **58**(3). 220-222.

[3] STAKHOV, Alexey Petrovich. *Introduction into algorithmic measurement theory*. Moscow: Soviet Radio, 1977.

[4] STAKHOV, Alexey Petrovich. The golden section in the measurement theory. *Computers Math. Applic.* 1989, **17**(4-6). 613-638.

[5] STAKHOV, Alexey Petrovich. A generalization of the Fibonacci Q-matrix. *Rep Nat Acad Sci Ukraine*. 1999(9). 46-9.

[6] KILIC, Emrah. The Binet formula, sums and representations of the generalized Fibonacci p-numbers. *Europepan Journal of Combinatorics*. 2008, **29**. 701-711.

[7] KILIC, Emrah, STAKHOV, Alexey Petrovich. *Chaos, Solitons and Fractals.* 2009, **40**. 2210-2221.

[8] KOCER, Gokcen, TUGLU, Naim, STAKHOV, Alexey Petrovich. On the m-extension of the Fibonacci and Lucas *p*-numbers. *Chaos, Solitons and Fractals.* 2009, **40**. 1890-1906.

[9] SPINADEL, Vera. *From the golden mean to chaos*. Nuveva Liberia, 1998.

[10] GAZALE, Midhat. *From pharaons to fractals. Princeton* (NJ): Princeton University Press, 1999.

[11] KAPRAFF, Jay. *Beyond measure. A guided tour through nature, myth, and number*. Sinagapore: World Scientific, 2002.

[12] STAKHOV, Alexey Petrovich. *Gazalae formulas, a new class of the hyperbolic Fibonacci and Lucas functions, and the improved method of the „golden" cryptography*. Moscow: Academy of Trinitarism. 2006, 77-6567.

[13] FALCON, Plaza. On the Fibonacci *k*-numbers. *Chaos, Solitons and Fractals.* 2007, **32**(5). 1615-24.

[14] FALCON, Plaza. The *k*- Fibonacci hyperbolic functions. *Chaos, Solitons and Fractals.* 2008, **38**(2). 409-420.

[15] TUGLU, Naim, KOCER, Gokcen, STAKHOV, Alexey Petrovich. *Bivariate fibonacci like p-polynomials. Applied Mathematics and Computation*. 2011, **217**. 10239-10246.

[16] STAKHOV, Alexey Petrovich. Fibonacci matrices, a generalization of the „Cassini fromula, and a new coding theory. *Chaos, Solitons and Fractals.* 2006, **30**. 56-66.

[17] STAKHOV, Alexey Petrovich. The „golden" matrices and a new kind of cryptography. *Chaos, Solitons and Fractals.* 2007, **32**. 1138-1146.

[18] BASU, Mansjuri, PRASAD, Bandhu. Coding theory on the m-extension of the Fibonacci p-numbers. *Chaos, Solitons and Fractals.* 2009, **42**. 2522-2530.

[19] BASU, Mansjuri, PRASAD, Bandhu. Coding theory on the (m,t)-extension of the Fibonacci p-numbers. *Chaos, Solitons and Fractals.* 2011, **3**(2). 259-267.

[20] BASU, Mansjuri, PRASAD, Bandhu. Coding theory on *h(x)* Fibonacci p-numbers polynomilas. *Discrete Mathematics, Algorithms and Apllications*. 2012, **4**(3).

[21] PRASAD, Bandhu. High rates of Fibonacci polynomilas coding theory. *Discrete Mathematics, Algorithms and Apllications.* 2014, **6**(4).