Jaromír Abrham; Miloslav Driml
O jednom problému z theorie kodování

Časopis pro pěstování matematiky, Vol. 81 (1956), No. 1, 69--76

Persistent URL: http://dml.cz/dmlcz/117173

Časopis pro pěstování matematiky, roč. 81 (1956)

O JEDNOM PROBLÉMU Z THEORIE KODOVÁNÍ

JAROMÍR ABRHAM, MILOSLAV DRIML, Praha.

(Došlo dne 15. února 1955.) DT: 621.39.001

V článku je podána methoda tvoření pětipísmenných kodových slov, z nichž každá dvě se liší alespoň na třech místech.

1. Úvod

Státní a obchodní telegramy se zasílají většinou kodovaně. Ponejvíce se používá s ohledem na sazební předpisy kodů s pětipísmennými slovy. K usnadnění luštění zkomolenin, ke kterým někdy při telegrafní přepravě dochází, vyžaduje se zpravidla, aby se kodová slova lišila mezi sebou v určitém počtu míst. Většina dosavadních kodů byla založena na principu dvoumístného rozlišení, jehož nevýhodou je, že nedovoluje jednoznačně vyluštit zkomoleninu, vzniklou na jednom místě; tuto potíž odstraňuje třímístné rozlišení kodových slov.

Slov s třímístným rozlišením bylo po prvé použito v „*Bentley's Second Phrase Code*" (1. vydání 1929) ke kodování čísel a peněžních částek; nejrozsáhlejší skupina takových slov tohoto kodu obsahuje však pouze 4052 takových slov z 26písmenné abecedy. Při tom není udán způsob tvoření těchto slov.

Výsledků obsažených v této práci bylo použito při sestavování kodových slov pro připravovaný kod Čs. obchodní komory *Unicode*.

Matematicky budeme formulovat problém tvoření kodových slov s třímístným rozlišením tímto způsobem:

Buďtež dány konečné uspořádané množiny $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_5$ o stejném počtu prvků rovném n. Kartézský součin $\mathfrak{M}_1 \times \mathfrak{M}_2 \times \ldots \times \mathfrak{M}_5$ obsahuje n^5 prvků tvaru $[\alpha_1, \alpha_2, \ldots, \alpha_5]$, kde $\alpha_i \in \mathfrak{M}_i$, $i = 1, 2, \ldots, 5$. Nadále budeme, jak je zvykem v theorii informací, nazývati množiny $\mathfrak{M}_i$, $i = 1, 2, \ldots, 5$, *abecedami*, jejich prvky *písmeny* a pětice z jejich kartézského součinu *slovy*. Budeme se zabývati otázkou, kolik lze vybrat slov tak, aby se každá dvě z nich lišila alespoň na třech místech. Takováto slova budeme nazývati slovy s třímístným rozlišením.

2. Dosažitelný počet slov s třímístným rozlišením

Věta 1. *Slov s třímístným rozlišením lze vybrat nejvýše* n^3.

Důkaz. Aby nenastala shoda na třech místech, musí se každá dvě slova lišit alespoň na jednom místě v libovolné uvažované trojici; takových slov při dané trojici existuje právě n^3.

Uvedená věta udává pouze horní hranici, kterou počet slov s třímístným rozlišením nemůže překročit. Tato hranice však není vždy dosažitelná. Je-li na př. $n = 2$, $\mathfrak{M}_i = \{A, B\}$ $(i = 1, 2, \ldots, 5)$, pak můžeme vytvořit nejvýše čtyři slova s třímístným rozlišením. Jsou to na př. slova $AAAAA$, $AABBB$, $BBAAB$, $BBBBA$. Vybereme-li však slova $AAAAA$, $BBBBB$, nebo libovolná jiná dvě slova, která se liší na všech pěti místech, zjistíme snadno, že k nim nemůžeme přidat žádné další slovo, zachovávající podmínku třímístného rozlišení. Odtud je zřejmé, že dosažitelný počet slov s třímístným rozlišením závisí na způsobu jejich vybírání. Je proto vhodné zavésti tuto definici:

Způsob vybírání kodových slov nazveme optimálním, vede-li k vybrání maximálního dosažitelného počtu slov.

Dalším naším úkolem bude nalézti optimální způsob vybírání slov s třímístným rozlišením.

3. Způsob tvoření slov s třímístným rozlišením

Vyjdeme ze systému pěti vedle sebe položených uspořádaných abeced $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_5$. Písmena každé z abeced očíslujeme čísly $0, 1, \ldots, n-1$. Budiž r celé nezáporné číslo menší než n. Budeme značit $\mathfrak{M}_i^{(r)}$ takovou cyklickou permutaci abecedy $\mathfrak{M}_i$, v níž na nultém místě stojí r-té písmeno původního uspořádání. Místo $\mathfrak{M}_i^{(0)}$ budeme ve shodě s dosavadním značením psáti pouze $\mathfrak{M}_i$. Jsou-li dána celá čísla a, b, c — nazveme je charakteristikami — taková, že $0 \leqq a, b, c \leqq n-1$ a probíhají-li s, t nezávisle čísla $0, 1, \ldots, n-1$, tvoříme slova takto:

Na prvé místo slova postavíme s-té písmeno abecedy $\mathfrak{M}_1$, na druhé místo s-té písmeno abecedy $\mathfrak{M}_2^{(a)}$, na třetí místo t-té písmeno abecedy $\mathfrak{M}_3$, na čtvrté místo t-té písmeno abecedy $\mathfrak{M}_4^{(b)}$, na páté místo q-té písmeno abecedy $\mathfrak{M}_5^{(c)}$, kde $q \equiv s + t \pmod{n}$, $0 \leqq q \leqq n-1$. (Symbol $\equiv$ zde značí kongruenci podle vyznačeného modulu.)

Tím dostáváme vzájemně jednoznačné přiřazení dvojic $(0, s)$, (a, s), $(0, t)$, (b, t), (c, q) a abeced $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_5$. Dále uvedené vlastnosti popsaného postupu se nezmění, nahradíme-li u abeced $\mathfrak{M}_i$ indexy $1, 2, \ldots, 5$ jejich libovolnou permutací.

Je zřejmé, že vyložený postup dovoluje při pevných hodnotách charakteristik a, b, c vytvoření n^2 slov, z nichž každá dvě se liší alespoň na třech místech.

Odvodíme nyní podmínky pro charakteristiky a, b, c, při jejichž splnění se slova utvořená za pomoci různých hodnot těchto charakteristik liší alespoň na třech místech.

Věta 2. *Nutnou a postačující podmínkou pro to, aby při dvou různých trojicích charakteristik a_1, b_1, c_1; a_2, b_2, c_2 neexistovala dvojice slov se shodou na třech místech je*

$$\begin{gathered} a_1 \not\equiv a_2 \pmod{n}, \quad b_1 \not\equiv b_2 \pmod{n}, \quad c_1 \not\equiv c_2 \pmod{n}, \\ a_1 - c_1 \not\equiv a_2 - c_2 \pmod{n}, \quad b_1 - c_1 \not\equiv b_2 - c_2 \pmod{n}, \\ a_1 + b_1 - c_1 \not\equiv a_2 + b_2 - c_2 \pmod{n}. \end{gathered} \tag{1}$$

Důkaz. Ke shodě na 1. a 2. místě slova nedojde tehdy a jen tehdy, když

$$a_1 \not\equiv a_2 \pmod{n}.$$

Tím je vyloučena možnost shody na 1., 2., 3.; 1., 2., 4. a 1., 2., 5. místě. Podobně ke shodě na 3. a 4. místě nedojde v žádné dvojici slov tehdy a jen tehdy, když

$$b_1 \not\equiv b_2 \pmod{n}.$$

Tím je vyloučena možnost shody na 1., 3., 4.; 2., 3., 4. a 3., 4., 5. místě. Uvážíme ještě zbývající možnosti. Ke shodě na 1., 3., 5. místě slova nedojde tehdy a jen tehdy, je-li

$$c_1 \not\equiv c_2 \pmod{n}.$$

Nesmí totiž být $c_1 + s + t \equiv c_2 + s + t \pmod{n}$. Prvním místem je však určeno číslo s, třetím místem číslo t.

Ke shodě na 1., 4., 5. místě dojde tehdy a jen tehdy, platí-li

$$s_1 = s_2, \quad b_1 + t_1 \equiv b_2 + t_2 \pmod{n}, \quad c_1 + s_1 + t_1 \equiv c_2 + s_2 + t_2 \pmod{n} \tag{2}$$

(s_i, t_i značí čísla s a t při charakteristikách a_i, b_i, c_i, $i = 1, 2$). Odtud vyplývá, že podmínka

$$b_1 - c_1 \equiv b_2 - c_2 \pmod{n}$$

je nutná k tomu, aby nastala shoda na 1., 4., 5. místě. Tato podmínka je také postačující. Je-li dáno 1., 4., 5. místo slova vytvořeného pomocí charakteristik a_1, b_1, c_1, jsou určena čísla s_1 a t_1. Zvolíme-li nyní

$$s_2 = s_1, \quad t_2 \equiv b_1 - b_2 + t_1 \pmod{n}, \quad 0 \leqq t_2 \leqq n - 1,$$

jsou splněny podmínky (2) a tedy nastane shoda na 1., 4., 5. místě.

Případ shody na 2., 3., 5. místě je obdobný předchozímu. Nutnou a postačující podmínkou shody dvou slov na těchto místech je platnost vztahů

$$\begin{gathered} a_1 + s_1 \equiv a_2 + s_2 \pmod{n}, \\ t_1 = t_2, \quad c_1 + s_1 + t_1 \equiv c_2 + s_2 + t_2 \pmod{n}. \end{gathered}$$

Stejně jako při shodě na 1., 4., 5. místě odvodíme nutnou a postačující podmínku

$$a_1 - c_1 \not\equiv a_2 - c_2 \pmod{n}$$

pro to, aby nemohla nastat uvažovaná shoda.

Zbývá shoda na 2., 4., 5. místě. Aby nastala, je nutné a stačí, aby platilo

$$a_1 + s_1 \equiv a_2 + s_2 \pmod{n}, \quad b_1 + t_1 \equiv b_2 + t_2 \pmod{n}, \quad (3)$$
$$c_1 + s_1 + t_1 \equiv c_2 + s_2 + t_2 \pmod{n}.$$

Sečtením prvních dvou kongruencí a odečtením třetí dostaneme nutnou podmínku

$$a_1 + b_1 - c_1 \equiv a_2 + b_2 - c_2 \pmod{n}$$

pro to, aby nastala taková shoda. Tato podmínka je také postačující. Je-li totiž dáno 2., 4., 5. místo slova utvořeného při charakteristikách a_1, b_1, c_1, jsou tím určena čísla s_1 a t_1. Zvolíme-li nyní

$$s_2 \equiv a_1 - a_2 + s_1 \pmod{n},$$
$$t_2 \equiv b_1 - b_2 + t_1 \pmod{n}$$

a platí-li

$$a_1 + b_1 - c_1 \equiv a_2 + b_2 - c_2 \pmod{n},$$

je tím dosaženo splnění podmínek (3). Tím je důkaz věty 2 zakončen.

Z věty 2 plyne, že pomocí k trojic a, b, c, z nichž každé dvě vyhovují podmínkám (1), lze utvořit právě $k \cdot n^2$ slov s třímístným rozlišením.

Pro další úvahy si zavedeme ještě toto označení:

Jsou-li p, q libovolná celá čísla, označíme (p, q) jejich největšího kladného společného dělitele. Speciálně $(p, q) = 1$ bude značit, že p, q jsou nesoudělná.

Pomocná věta. *Jsou-li p, q, r libovolná celá čísla, pak alespoň jedno z čísel $p, q, r, p - r, q - r, p + q - r$*

a) je dělitelno dvěma,

b) je dělitelno třemi.

Důkaz. a) Jsou-li všechna tři čísla p, q, r lichá, jsou čísla $p - r$ i $q - r$ sudá.

b) Nechť $(p, 3) = (q, 3) = (r, 3) = (p - r, 3) = q - r, 3) = 1$. Dokážeme, že potom $(p + q - r, 3) = 3$. Čísla p, q, r určují jednoznačně čísla $\bar{p}, \bar{q}, \bar{r}$ taková, že $\bar{p} \equiv p \pmod 3$, $\bar{q} \equiv q \pmod 3$, $\bar{r} \equiv r \pmod 3$ a že každé z čísel $\bar{p}, \bar{q}, \bar{r}$ je rovno jedné nebo dvěma. Aby bylo $(p - r, 3) = (q - r, 3) = 1$, musí být $\bar{p} = \bar{q} \neq \bar{r}$. Potom však je

$$p + q - r \equiv \bar{p} + \bar{q} - \bar{r} \equiv 0 \pmod 3.$$

Věta 3. *Nechť $(n, 2) = (n, 3) = 1$. Potom existuje n trojic a_k, b_k, c_k $(k = 1, 2, \ldots, n)$, z nichž každé dvě vyhovují podmínkám věty 2; je tedy pro taková n výše popsaný způsob vybírání slov optimální.*

Důkaz. Zvolme přirozená čísla d_1, d_2, d_3 taková, že

$$(d_i, n) = 1, \quad 1 \leq d_i \leq n - 1, \quad i = 1, 2, 3$$

a že

$$(d_1 - d_3, n) = (d_2 - d_3, n) = (d_1 + d_2 - d_3, n) = 1.$$

(Taková d_i, $i = 1, 2, 3$, skutečně existují; stačí volit na př. $d_1 = d_2 = 2$, $d_3 = 1$.) Buďtež a_1, b_1, c_1 libovolná čísla ležící mezi čísly $0, 1, \ldots, n - 1$. Definujme

$$a_k \equiv a_1 + (k-1)\, d_1 \pmod{n}, \quad b_k \equiv b_1 + (k-1)\, d_2 \pmod{n},$$
$$c_k \equiv c_1 + (k-1)\, d_3 \pmod{n}$$

tak, aby bylo

$$0 \leqq a_k \leqq n-1, \quad 0 \leqq b_k \leqq n-1, \quad 0 \leqq c_k \leqq n-1, \quad k = 1, 2, \ldots, n.$$

Potom

$$a_k - c_k \equiv a_1 - c_1 + (k-1)(d_1 - d_3) \pmod{n},$$
$$b_k - c_k \equiv b_1 - c_1 + (k-1)(d_2 - d_3) \pmod{n},$$
$$a_k + b_k - c_k \equiv a_1 + b_1 - c_1 + (k-1)(d_1 + d_2 - d_3) \pmod{n}.$$

Pro libovolné celé číslo r označme r^* takové číslo, pro něž platí $r^* \equiv r \pmod{n}$, $0 \leqq r^* \leqq n-1$. Potom n-členné posloupnosti $\{a_k\}$, $\{b_k\}$, $\{c_k\}$, $\{(a_k - c_k)^*\}$, $\{(b_k - c_k)^*\}$, $\{(a_k + b_k - c_k)^*\}$ probíhají všechna celá čísla $0, 1, \ldots, n-1$.

Dokážeme toto tvrzení v obecném tvaru: Budiž dáno přirozené číslo d takové, že $(d, n) = 1$, $1 \leqq d \leqq n-1$. Definujme $m_k = m_1 + (k-1)\, d$, $k = 1, 2, \ldots, n$, kde m_1 je libovolné celé číslo, splňující nerovnost $0 \leqq m_1 \leqq n-1$. Pak se v konečné posloupnosti $m_1, m_2^*, \ldots, m_n^*$ vyskytuje každé z čísel $0, 1, \ldots, n-1$ právě jednou.

Předpokládejme, že by tomu tak nebylo. Pak existují indexy k, l, $1 \leqq k < l \leqq n$ tak, že $m_k^* = m_l^*$, tedy $m_1 + (k-1)\, d \equiv m_1 + (l-1)\, d \pmod{n}$; jelikož $(d, n) = 1$, dostáváme odtud po snadné úpravě

$$l \equiv k \pmod{n},$$

což je ve sporu s předpokladem.

Je-li n dělitelno třemi, věta 3 neplatí; zvolíme-li na př. $n = 3$, pak podle pomocné věty před větou 3 snadno zjistíme, že k žádné trojici charakteristik a, b, c nemůžeme přidat další trojici, splňující podmínky (1). Vede tedy v tomto případě popsaný způsob k vybrání devíti slov; bylo však pokusnou cestou zjištěno, že takových slov lze vybrat alespoň osmnáct. Pro $n = 2$ je uvedený způsob optimální, zůstává však otevřenou otázkou, je-li optimální i při jiných sudých hodnotách čísla n. Způsobem popsaným v důkazu věty 3 nelze dosáhnout n^3 slov, je-li n sudé nebo dělitelno třemi. To vyplývá bezprostředně z pomocné věty.

Ukážeme ještě, že v případě, kdy $n = 2k$, kde k je liché číslo, nelze nalézt n trojic a_i, b_i, c_i, splňujících podmínky (1). Předpokládejme, že takové trojice existují. Pak mezi čísly a_i je právě k čísel lichých a k čísel sudých. Totéž platí i o číslech c_i. Jelikož n je sudé, jsou všechna čísla spolu kongruentní mod n současně lichá nebo současně sudá. Aby mohly být splněny podmínky (1), musí mezi čísly $a_i - c_i$ být k čísel sudých a k čísel lichých. Číslo $a_i - c_i$ je zřejmě liché tehdy a jen tehdy, je-li právě jedno z čísel a_i, c_i liché. Předpokládejme, že

v m trojicích a_i, b_i, c_i je a_i liché a c_i sudé. Pak musí být v $k - m$ trojicích a_i sudé a c_i sudé, v $k - m$ trojicích a_i liché i c_i liché a v m trojicích a_i sudé a c_i liché; je tedy právě ve $2m$ případech $a_i - c_i$ liché. Musí proto být $k = 2m$, což je ve sporu s předpokladem, že k je liché.

Резюме

ОБ ОДНОЙ ПРОБЛЕМЕ ИЗ ТЕОРИИ КОДИРОВАНИЯ

ЯРОМИР АБРГАМ, МИЛОСЛАВ ДРИМЛ (Jaromír Abrham, Miloslav Driml), Прага.

(Поступило в редакцию 15/II 1955 г.)

Даны конечные упорядоченные множества $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_5$ с одинаковым числом элементов, равным n. Эти множества мы будем называть *алфавитами*, их элементы *буквами*, а элементы декартова произведения этих множеств — *словами*. В работе разбирается вопрос о том, сколько можно подобрать таких слов, которые отличаются друг от друга по крайней мере на трех местах (такие слова мы назовем словами с трехместным различием).

В § 2 доказывается (теорема 1), *что можно подобрать не более* n^3 *таких слов*, причем эта граница не всегда достижима, и что достижимое число слов зависит от способа их подбора. Способ, позволяющий подобрать наибольшее достижимое количество таких слов, мы называем поэтому оптимальным.

В § 3 описывается метод подбора слов. Мы исходим из системы пяти расположенных друг около друга упорядоченных алфавитов $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \ldots, \mathfrak{M}_5$. Буквы каждого из алфавитов занумеруем числами $0, 1, \ldots, n-1$. Обозначим через $\mathfrak{M}_i^{(r)}$ такую циклическую перестановку алфавита $\mathfrak{M}_i$, в которой на нулевом месте стоит r-я буква ($r = 0, 1, \ldots, n-1$) первоначальнаго расположения букв алфавита. Если даны целые числа a, b, c — назовем их характеристиками — такие, что $0 \leqq a, b, c \leqq n-1$, и если s, t пробегают независимо друг от друга числа $0, 1, \ldots, n-1$, то мы образуем слова следующим образом:

На первое место слова поставим s-ю букву алфавита $\mathfrak{M}_1^{(0)}$, на второе место s-ю букву алфавита $\mathfrak{M}_2^{(a)}$, на третье место t-ю букву алфавита $\mathfrak{M}_3^{(0)}$, на четвертое место t-ю букву алфавита $\mathfrak{M}_4^{(b)}$, на пятое место q-ю букву алфавита $\mathfrak{M}_5^{(c)}$, где $q \equiv s + t \pmod{n}$, $0 \leqq q \leqq n-1$. (Символ $\equiv$ обозначает здесь сравнение по указанному модулю.) Таким образом мы образуем при фиксированных значениях характеристик a, b, c n^2 слов с трехместным различием.

Теорема 2. *Необходимым и достаточным условием для того, чтобы при двух различных тройках характеристик* a_1, b_1, c_1; a_2, b_2, c_2 *не могла существовать пара слов с тремя совпадающими местами, является справедливость соотношений*

$$\begin{gathered} a_1 \not\equiv a_2 \pmod{n}, \quad b_1 \not\equiv b_2 \pmod{n}, \quad c_1 \not\equiv c_2 \pmod{n}, \\ a_1 - c_1 \not\equiv a_2 - c_2 \pmod{n}, \quad b_1 - c_1 \not\equiv b_2 - c_2 \pmod{n}, \\ a_1 + b_1 - c_1 \not\equiv a_2 + b_2 - c_2 \pmod{n}. \end{gathered} \tag{1}$$

Обозначим теперь для любых целых чисел p, q символом (p, q) их общий положительный наибольший делитель.

Далее имеет место

Теорема 3. *Пусть* $(n, 2) = (n, 3) = 1$. *Тогда существует* n *троек* a_i, b_i, c_i, $i = 1, 2, \ldots, n$, *из которых любые две удовлетворяют условиям* (1); *следовательно, для таких* n *троек описанный выше способ подбора слов является оптимальным.*

На примере далее показано, что для n, делимого на три, теорема 3 несправедлива.

В заключение § 3 доказано, что если $n = 2k$, где k нечетно, то никоим образом нельзя найти n троек a_i, b_i, c_i, удовлетворяющих условиям (1).

Zusammenfassung

ÜBER EIN PROBLEM DER KODENTHEORIE

JAROMÍR ABRHAM, MILOSLAV DRIML, Praha.

(Eingelangt 15. 2. 1955.)

Es sind endliche geordnete Mengen $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_5$ mit derselben Anzahl von Elementen gleich n gegeben. Die Mengen werden wir weiter *Alphabete*, ihre Elemente *Buchstaben* und die Elemente aus ihrem kartesischen Produkt *Wörter* bezeichnen. In der Arbeit wird die Frage studiert, wieviel solche Wörter ausgewählt werden können, die sich wenigstens auf drei Stellen unterscheiden würden. Diese Wörter werden als „Wörter mit dreistelligem Unterschied" bezeichnet.

In § 2 wird bewiesen (Satz 1), *dass es möglich ist, höchstens* n^3 *solcher Wörter auszuwählen,* wobei aber diese Grenze nicht immer erreichbar ist und die maximal erreichbare Anzahl solcher Wörter von der Methode ihrer Auswahl abhängig ist. Die Methode, die zur höchsten erreichbaren Anzahl solcher Wörter führt, wird daher als die optimale bezeichnet.

In § 3 wird die Methode der Auswahl von Wörtern beschrieben. Wir werden

von einem System von fünf nebeneinander liegenden geordneten Alphabete $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_5$ ausgehen. Die Buchstaben jedes Alphabets werden mit den Nummern $0, 1, \ldots, n-1$ nummeriert. Wir werden eine solche zyklische Permutation des Alphabets $\mathfrak{M}_i$, in der an der nullten Stelle der r-te Buchstabe der ursprünglichen Anordnung steht, als $\mathfrak{M}_i^{(r)}$ bezeichnen. Wenn die ganzen Zahlen a, b, c (Charakteristiken genannt) gegeben sind, wobei $0 \leqq a, b, c \leqq n-1$ gilt und wenn s, t unabhängig voneinander die Zahlen $0, 1, \ldots, n-1$ durchlaufen, bilden wir die Wörter mit Hilfe der folgenden Methode:

An die erste Stelle des Wortes stellen wir den s-ten Buchstaben des Alphabets $\mathfrak{M}_1^{(0)}$, an die zweite Stelle den s-ten Buchstaben des Alphabets $\mathfrak{M}_2^{(a)}$, an die dritte Stelle den t-ten Buchstaben des Alphabets $\mathfrak{M}_3^{(0)}$, an die vierte Stelle den t-ten Buchstaben des Alphabets $\mathfrak{M}_4^{(b)}$, an die fünfte Stelle den q-ten Buchstaben des Alphabets $\mathfrak{M}_5^{(c)}$, wobei $q \equiv s + t \pmod{n}$ und $0 \leqq q \leqq n-1$ ist. (Der Symbol $\equiv$ bezeichnet hier die Kongruenz nach dem angegebenen Modul.) Derart werden n^2 Wörter mit dreistelligem Unterschied gebildet.

Weiter wird in § 3 der folgende Satz bewiesen:

Satz 2. *Die notwendige und hinreichende Bedingung, dass bei zwei verschiedenen Zahlentripeln der Charakteristiken a_1, b_1, c_1; a_2, b_2, c_2 nicht ein Paar Wörter existieren möchte, die an drei Stellen einen gemeinsamen Buchstaben hätten, ist die Gültigkeit der Beziehungen*

$$\begin{gathered} a_1 \not\equiv a_2 \pmod{n}, \quad b_1 \not\equiv b_2 \pmod{n}, \quad c_1 \not\equiv c_2 \pmod{n}, \\ a_1 - c_1 \not\equiv a_2 - c_2 \pmod{n}, \quad b_1 - c_1 \not\equiv b_2 - c_2 \pmod{n}, \\ a_1 + b_1 - c_1 \not\equiv a_2 + b_2 - c_2 \pmod{n}. \end{gathered} \tag{1}$$

Wir werden nun für beliebige ganze Zahlen p, q ihren grössten positiven gemeinsamen Teiler mit dem Symbol (p, q) bezeichnen.

Weiter gilt

Satz 3. *Lassen wir $(n, 2) = (n, 3) = 1$ gelten. Dann existieren n Zahlentripel a_k, b_k, c_k, $k = 1, 2, \ldots, n$, wobei immer zwei davon die Bedingungen (1) erfüllen. Die oben beschriebene Methode der Auswahl der Wörter ist also für diese Werte von n optimal.*

Auf einem Beispiel wird weiter gezeigt, dass für n, das durch drei teilbar ist, der Satz 3 nicht gilt.

Am Ende des § 3 wird bewiesen, dass es für den Fall $n = 2k$ (k eine ungerade Zahl) nicht möglich ist n Zahlentripel a_i, b_i, c_i, $i = 1, 2, \ldots, n$ zu bilden, die die Bedingungen (1) erfüllen.