Šifry a další způsoby reprezentace v barokní matematice

Miroslava Otavová

Katedra matematiky
VŠE Praha
otavova@vse.cz

XIV. seminář z historie matematiky pro vyučující na středních školách
Poděbrady
19.8. – 22.8.2019

Změna paradigmatu v 17. století

krize stávajících kulturních a společenských institucí
ztráta náboženské jednoty vedla k vypuknutí třicetileté války

ve vědě zpochybněna možnost všeobecně platného uchopení skutečnosti

touha po řádu a zvládnutí chaosu ve světě vede k revizi výchozích principů
universální nástroj poznání ve všech oborech mají poskytnout formální disciplíny, zvláště logika a matematika

Změna paradigmatu v 17. století

charakteristickým projevem barokní mentality je sázka na racionalitu a víra v neomezené možnosti lidského rozumu

pokusy vytvořit dokonalý jazyk, který by

- umožnil jednoznačné a přesné formulace
- byl způsobilý objektivně popsat skutečnost
- racionálním způsobem formulovat a řešit vzniklé otázky

Jan Caramuel z Lobkovic

jeden z posledních evropských polyhistorů a typický barokní kosmopolita
rodinné kořeny spojeny s rudolfinskou Prahou

1606 narozen v Madridu
otec Vavřinec Caramuel původně císařský matematik a astronom na dvoře Rudolfa II.
matka Kateřina de Vries, vnučka Jana Popela z Lobkovic

zázračné dítě, otec rozpoznal a rozvíjel jeho matematické nadání
od deseti let studium filosofie na universitě v Alcale, kde přetrvával vliv arabské kultury a byla aktivní také židovská menšina
Caramuelovo osudové seznámení s kabalou – celoživotní inspirace

Kabala

středověký proud hebrejského mysticismu založený na studiu bible
vypracoval tradici výkladu tóry, který stvoření světa chápe jako jazykový jev

myšlenka paralelismu jazykové struktury a struktury skutečnosti:
vznikl-li svět stvořitelským slovem Božím (tj. pomocí písmen abecedy), lze předpokládat, že jazyk odráží, dokonce vytváří strukturu universa
to opravňuje pokus vytvořit jazyk, který může napodobit akt stvoření

(princip kompozicionality má původ v kabale!)

Kabala

aparát kabaly je v podstatě matematické, přesněji kombinatorické povahy
hebrejská abeceda obsahuje 22 písmen (pouze souhlásky), které zároveň označují číslice

metody

- gematrie – umožňuje komparovat slova s odlišným významem a stejným ciferným součtem
- anagram – možnost vytvářet z daného slova slova nová pomocí permutací, přesmyčka
- ars notoria – jeden text je nositelem dalšího, skrytého textu

Jan Caramuel z Lobkovic

po absolvování filosofie v Alcale pokračoval studiem teologie na universitě v Salamance
1625 ještě za studií vstoupil do cisterciáckého řádu v klášteře La Espina
vyučování na řádových školách ve Španělsku a Portugalsku

1635 představenými vyslán na teologickou fakultu do Lovaně ve Španělském Nizozemí
vynikal elegantní a výstižnou logickou argumentací, působil však exaltovaně
1638 doktorát teologie
1641 zvrátil výsledek universitní disputace mezi jansenisty a jezuity – uznání papežského nuncia Fabia Chigiho

Jan Caramuel z Lobkovic

již na začátku lovaňského období vydal tiskem spis *Steganographia*, který přináší myšlenku šifrovacího klíče
evropská odezva, 1646 povolán císařem Ferdinandem III. do Prahy
zásluha na podepsání mírové smlouvy na jednání Vestfálského kongresu
generálním vikářem kardinála Harracha a opatem kláštera v Emauzích
postupný nárůst animozity v českém prostředí
v udání do Říma Caramuel označen jako *subiectum inquietum*

v Praze vytvořil a 1654 v Kolíně nad Rýnem vydal zásadní dílo *Theologia rationalis* věnované analýze jazyka

Jan Caramuel z Lobkovic

Jan Caramuel z Lobkovic

1657 jmenován novým papežem Alexandrem VII. (Fabio Chigi)
biskupem Satrijsko - Campagneské diecéze v jižní Itálii
bohatá intelektuální aktivita, vlastní biskupská tiskárna

- spis věnovaný novým neznámým možnostem šifrování
- učebnice základů čínské mluvnice
- nejrozsáhlejší matematické dílo *Mathesis biceps vetus et nova*

1673 biskupem diecéze ve Vigevanu
zemřel 1682
jeho hrob dodnes ve vigevanské katedrále

Steganografie – koncepce šifrovacího klíče

Steganographiae facilis dilucidatio, declaratio etc. je komentovaná edice starého renesančního textu opata Jana Trithemia, OSB (+1516) původně vydán z pozůstalosti pod názvem *Polygraphia* v roce 1606 1609 zařazen na index zakázaných knih

autor otevřeně deklaruje svoji inspiraci židovskou kabalou
výrazně magická dikce, pasáže formálního charakteru (využití kombinatoriky) střídá vzývání démonů
zkušený teolog Caramuel byl schopen oddělit obsah a dráždící podání zrušil tabu – odborná veřejnost se mohla začít legitimně zabývat tématem

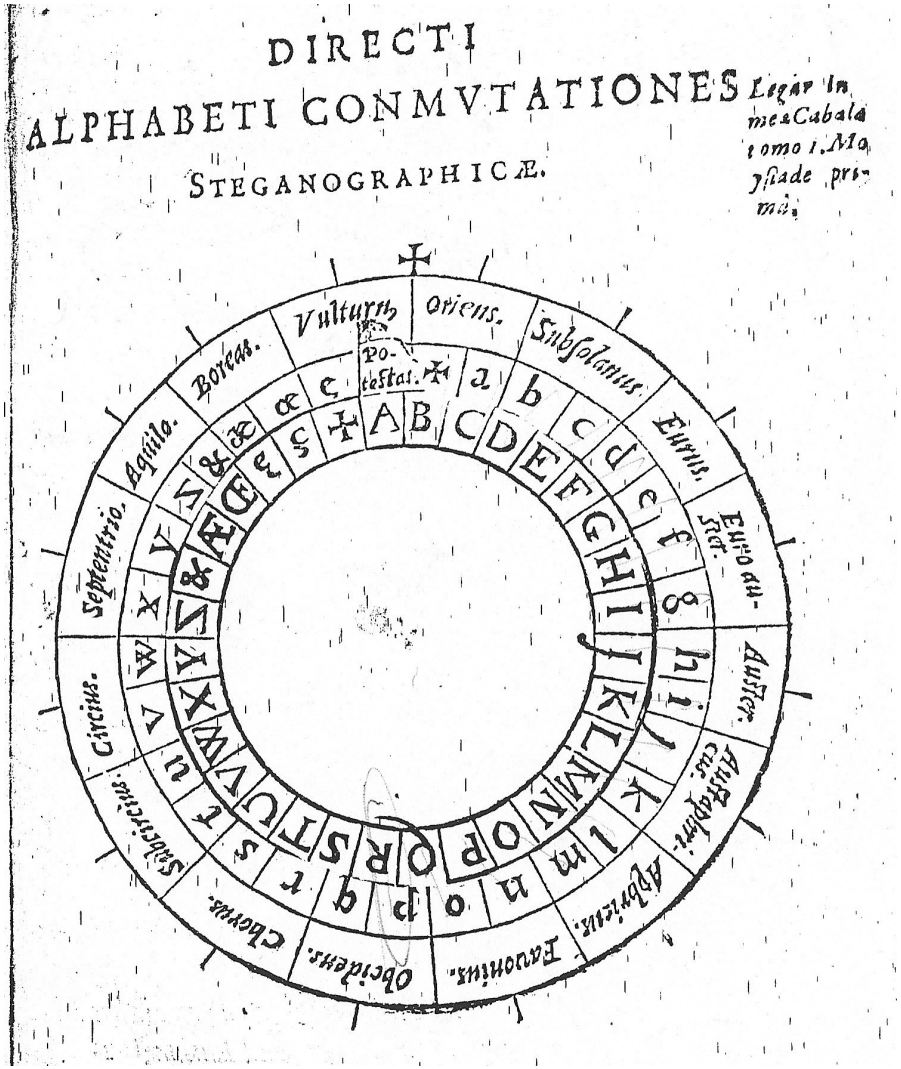
Steganografie – koncepce šifrovacího klíče

šifrovací algoritmy – obecné procesy, které lze specifikovat konkrétní volbou šifrovacího klíče
prostředky kombinatoriky lze popsat, kolik různých šifrovacích klíčů algoritmus poskytuje
jejich počet nepřímo úměrný riziku, že šifrovaný text bude dekódován

Caramuela zajímal i opačný problém – dešifrování, tzv. *anoigografie* (z řeckého *anoigó* – odhaluji vs. *steganos* – neproniknutelný)
otázku odhalení smyslu zašifrovaného textu pojímal ve větší obecnosti

v dalších spisech došel až k úvahám o možnosti vytvoření umělého jazyka

Šifrovací kotouč – *character* vs. *potestas*



Theologia rationalis (1645)

nejzávažnější dílo Caramuelova pražského působení
navzdory názvu jde o spekulativní gramatiku, analýzu jazyka prováděnou prostředky matematiky a logiky
připomíná metody logického pozitivismu 19. a 20. století

oddíl *Grammatica audax* (Odvážná mluvnice) – prostředky kombinatoriky zjednává hlubší vhled do logické struktury soudobé latiny, adaptuje ji pro potřeby vědeckého zkoumání

prostředky čistě logické – zjemnění významu kvantifikátorů
na úrovni sémantické precizuje významy zaváděním uměle vytvořených sloves
vytváří tzv. metafyzický dialekt

Theologia rationalis (1645)

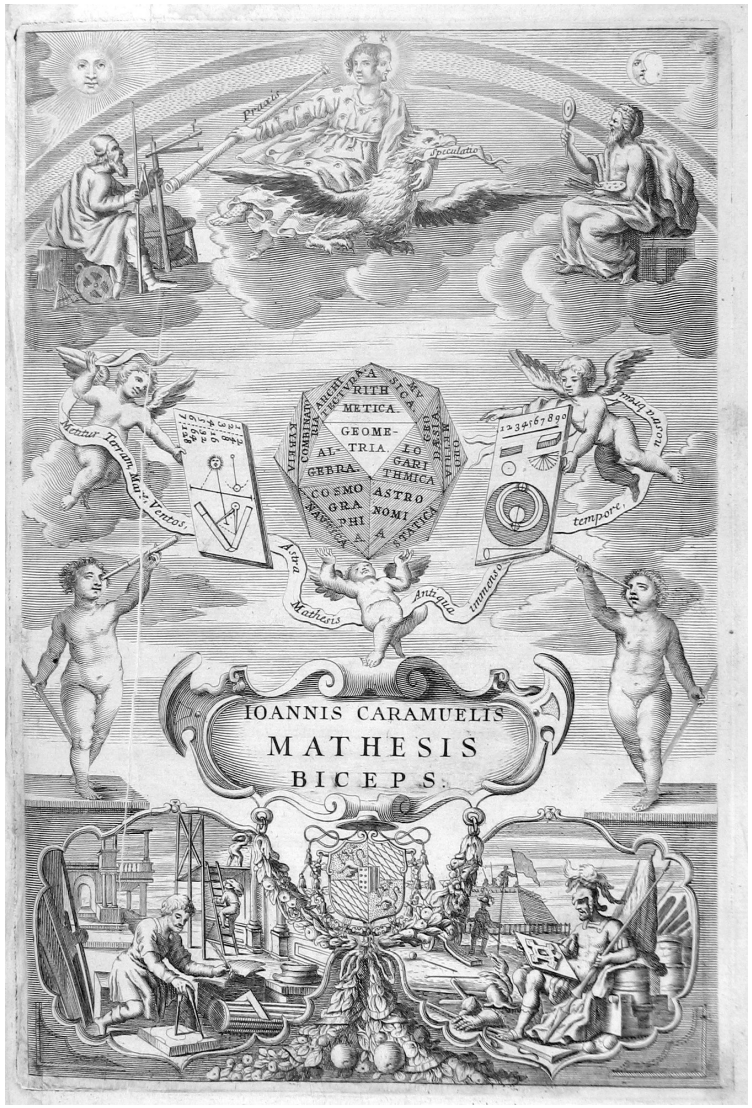
Mathesis biceps (1667, 1669)

programové propojení teorie a praktických aplikací matematiky
encyklopedický spis ve dvou svazcích vydán ve vlastní tiskárně v Campanii

- *Mathesis biceps vetus et nova* (1667)
- *Mathesis nova* (1669)

tisk foliového formátu, rozsah více než 1700 stran, navíc 52 stran obrazových příloh, podrobný obsah a věcný rejstřík, kvalitní grafická úprava, u obou svazků titulní listy s celostránkovými rytinami

Mathesis biceps vetus et nova (1667)



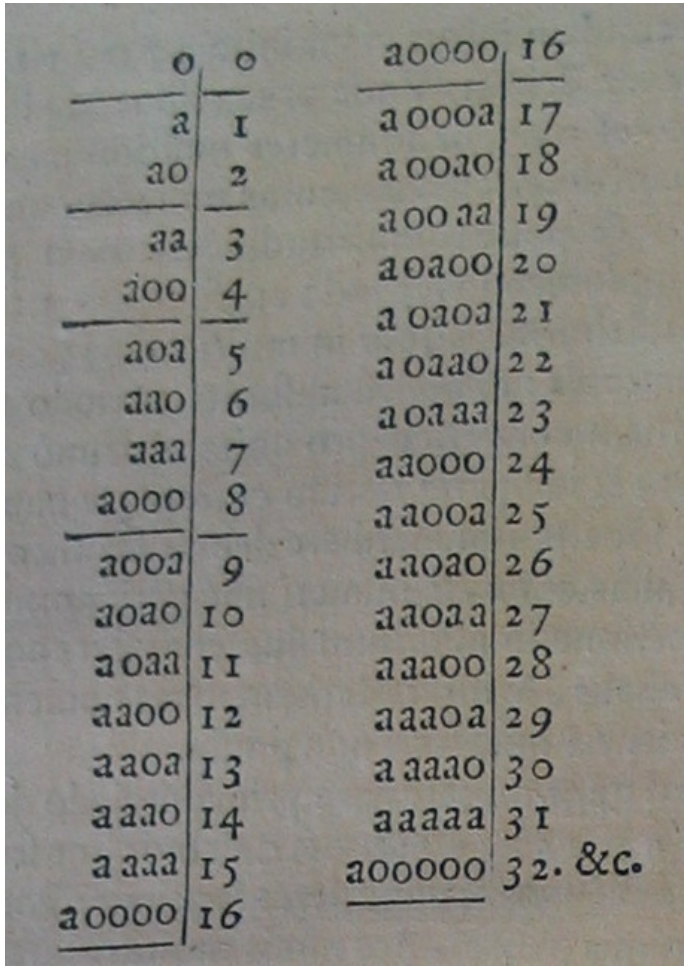
Mathesis biceps vetus et nova (1667) – detail

Pojetí aritmetiky a algebry

využívá zkušeností ze studia jazyka, konkrétně spekulativní gramatiky

Proarithmetica – propedeutická disciplína, postuluje filosofické základy
definice pojmu čísla – má instrumentální povahu
různé konkrétní reprezentace čísla,tedy ve skutečnosti více aritmetik
zavedení různých číselných soustav
Caramuel rozebírá binární, ternární, kvaternární, obecně n-ární aritmetiku pro $n = 2, 3, \ldots, 10, 12, 60$
pro reprezentaci užívá písmena *o, a, b, c, . . .* , tedy n navzájem různých znaků

Reprezentace binární aritmetiky



0	0
a	1
ao	2
aa	3
aoo	4
aoa	5
aao	6
aaa	7
aooo	8
aooa	9
aoao	10
aoaa	11
aaoo	12
aaoa	13
aaao	14
aaaa	15
aoooo	16

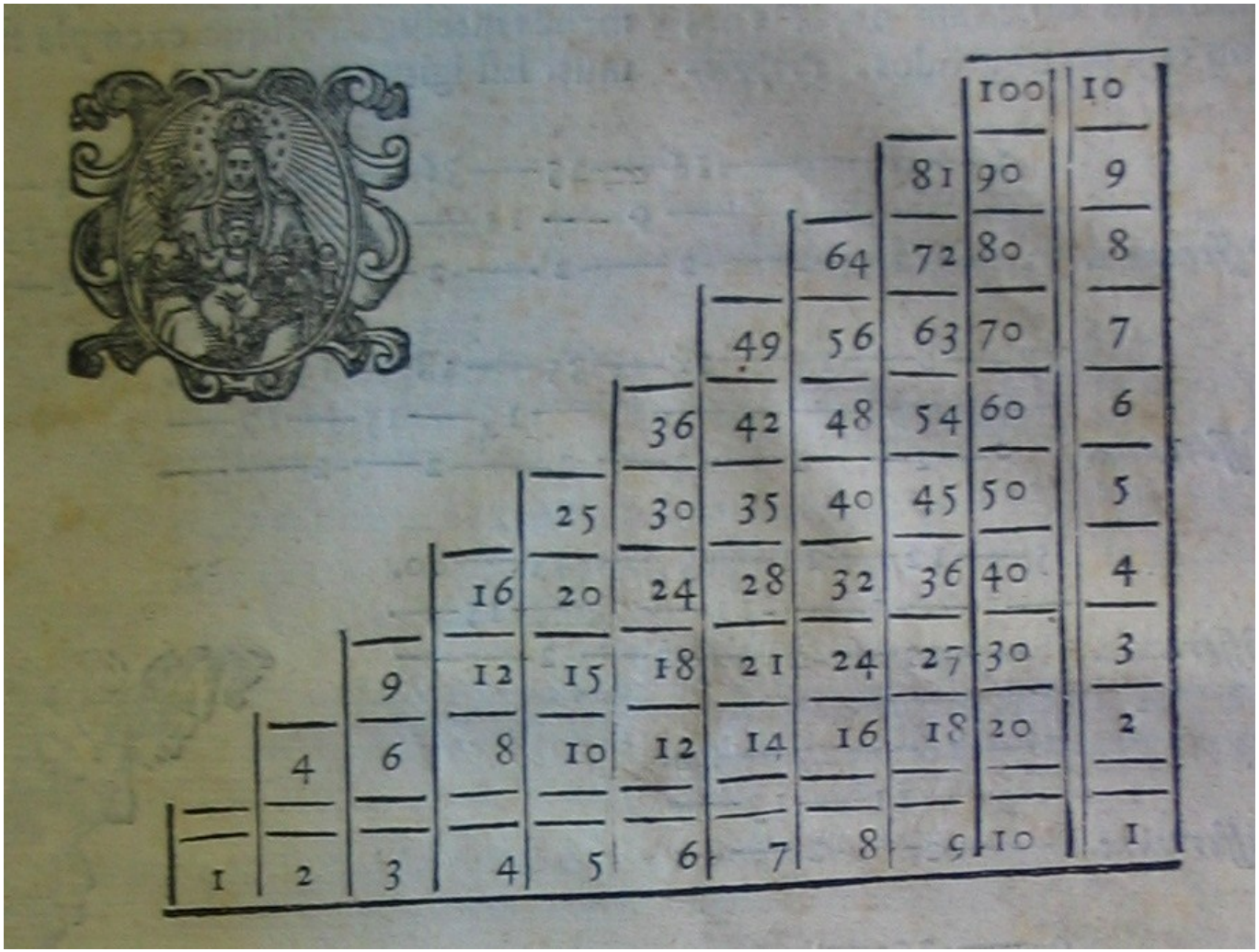
aoooo	16
aoooa	17
aooao	18
aooaa	19
aoaoo	20
aoaoa	21
aoaao	22
aoaaa	23
aaooo	24
aaooa	25
aaoao	26
aaoaa	27
aaaoo	28
aaaoa	29
aaaao	30
aaaaa	31
aooooo	32. &c.

Pojetí aritmetiky a algebry

Synarithmetica (techné arithmetiké, numerandi ars)
studuje aritmetické operace s čísly nezávisle na jejich konkrétní reprezentaci
technika výpočtu popsána obecně
ukázky v desítkové, ale i v jiných číselných soustavách

kromě čtyř základních operací metoda *Regula Aurea* včetně aplikací v obchodním podnikání
metody výpočtu druhé a třetí odmocniny
algoritmy usnadňující technicky náročné výpočty využitím tabulky *Scala Pythagorae*

Scala Pythagorae



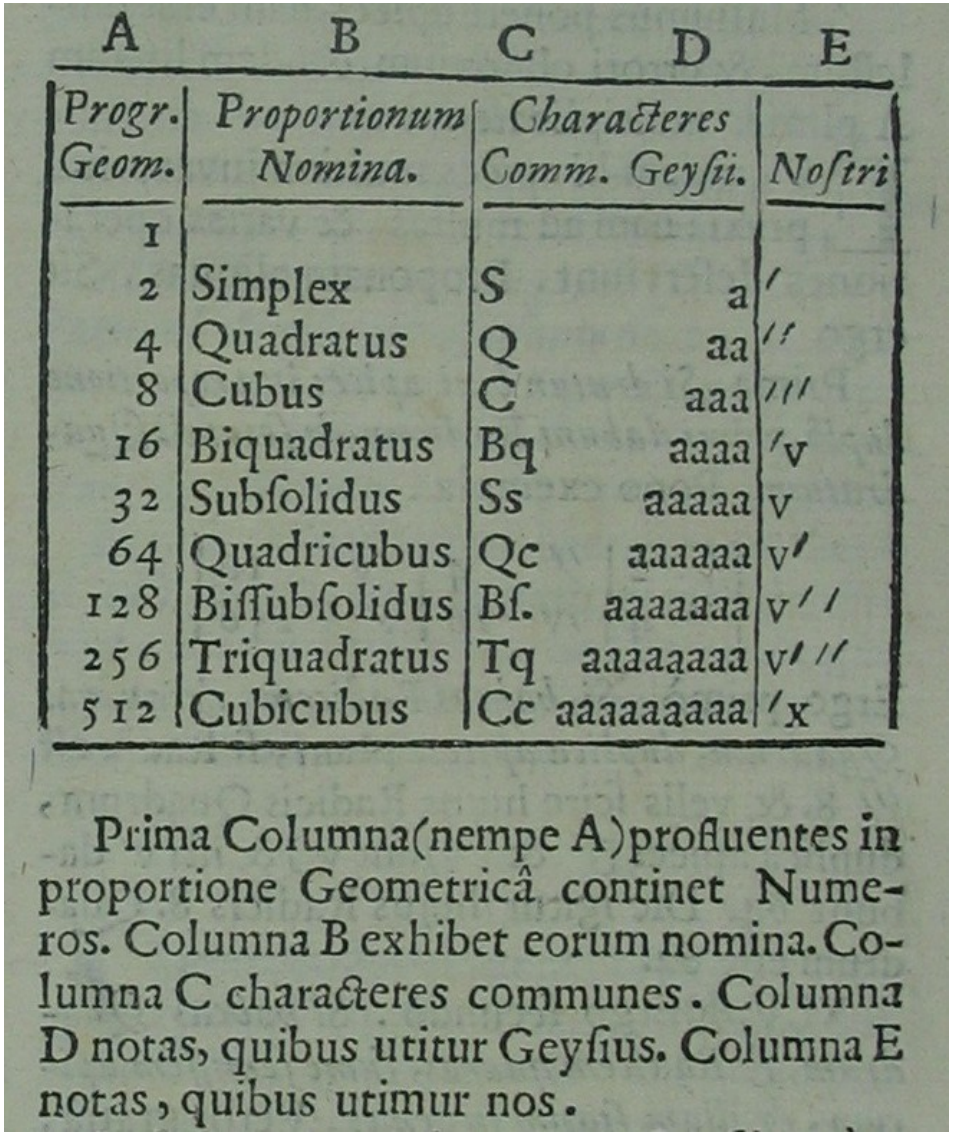
Pojetí aritmetiky a algebry

Metarithmetica neboli algebra

koncept proměnné, v textu zvané *numerus hypotheticus* nebo též *numerus tantuslibet*
esenciálním objektem algebry číslo *artificiální* (v dnešní dikci vlastně algebraický výraz), které je vyjádřením poměru, tj. závislosti na proměnné
akcidentálním objektem algebry je pak konkrétní jednoznačně určená hodnota

Caramuel užívá symboly (*character*) již velice blízké modernímu značení
matematický zápis chápe jako univerzální jazykový fenomén

Caramuelovo značení mocnin v algebře



A	B	C	D	E
Progr. Geom.	*Proportionum Nomina.*	*Characteres Comm.*	*Geyſii.*	*Noſtri*
1				
2	Simplex	S	a	′
4	Quadratus	Q	aa	′′
8	Cubus	C	aaa	′′′
16	Biquadratus	Bq	aaaa	′v
32	Subſolidus	Ss	aaaaa	v
64	Quadricubus	Qc	aaaaaa	v′
128	Biſſubſolidus	Bſ.	aaaaaaa	v′′
256	Triquadratus	Tq	aaaaaaaa	v′′′
512	Cubicubus	Cc	aaaaaaaaa	′x

Prima Columna (nempe A) profluentes in proportione Geometricâ continet Numeros. Columna B exhibet eorum nomina. Columna C characteres communes. Columna D notas, quibus utitur Geyſius. Columna E notas, quibus utimur nos.

Kombinatorika

pro Caramuela speciální případ aritmetiky

etymologie pojmu – kombinatorika sensu stricto (*Combinatoria*)
studuje kombinace, v latině spojování do dvojic
zabývá se problémem, kolik dvojic (*binario*) lze určitým přesně definovaným způsobem vytvořit z daného počtu prvků

v případě trojic, čtveřic, atd. by tedy adekvátním pojmem měla být *Comtrinatoria*, *Conquaternatoria*, atd.

s ohledem na záměr vybudovat obecnou teorii pro libovolnou délku k vytvářené skupiny však autor nadále používá slovo *Combinatoria* v dnešním smyslu

Kombinatorika

definice různých způsobů kombinací, tj. vytváření k-tic z daného počtu prvků
klasifikace vychází ze scholastické terminologie a uvádí základní tři možnosti

- rozlišení podle substance (zohledňuje různost přítomných prvků)
- podle pozice (zohledňuje jejich uspořádání)
- podle opakování

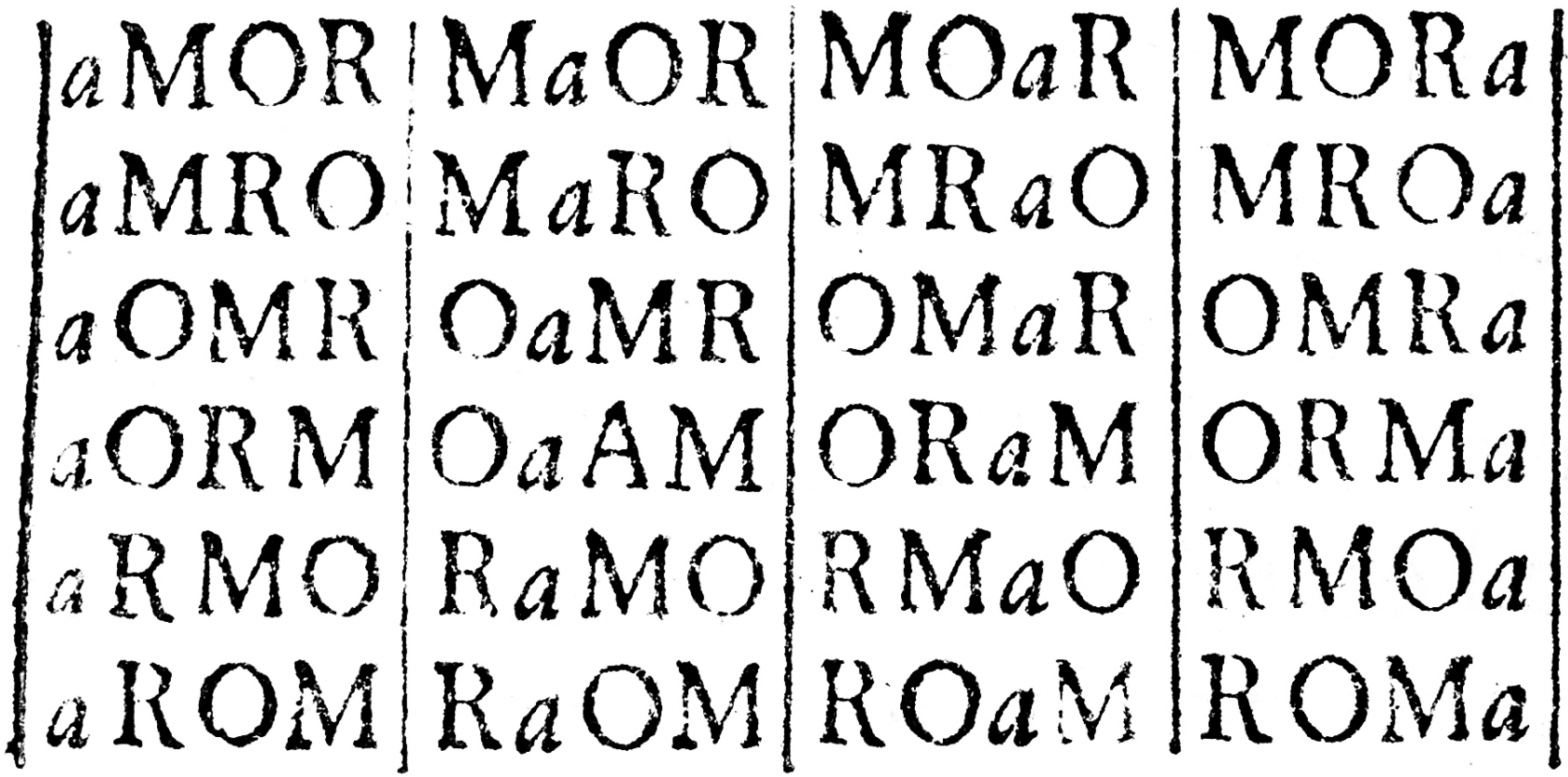
Caramuelova terminologie neodpovídá současné, ale uplatněním jedné nebo více uvedených diferencí z dnešního pohledu postupně studuje kombinace, variace i permutace jak bez opakování, tak s opakováním

Kombinatorika

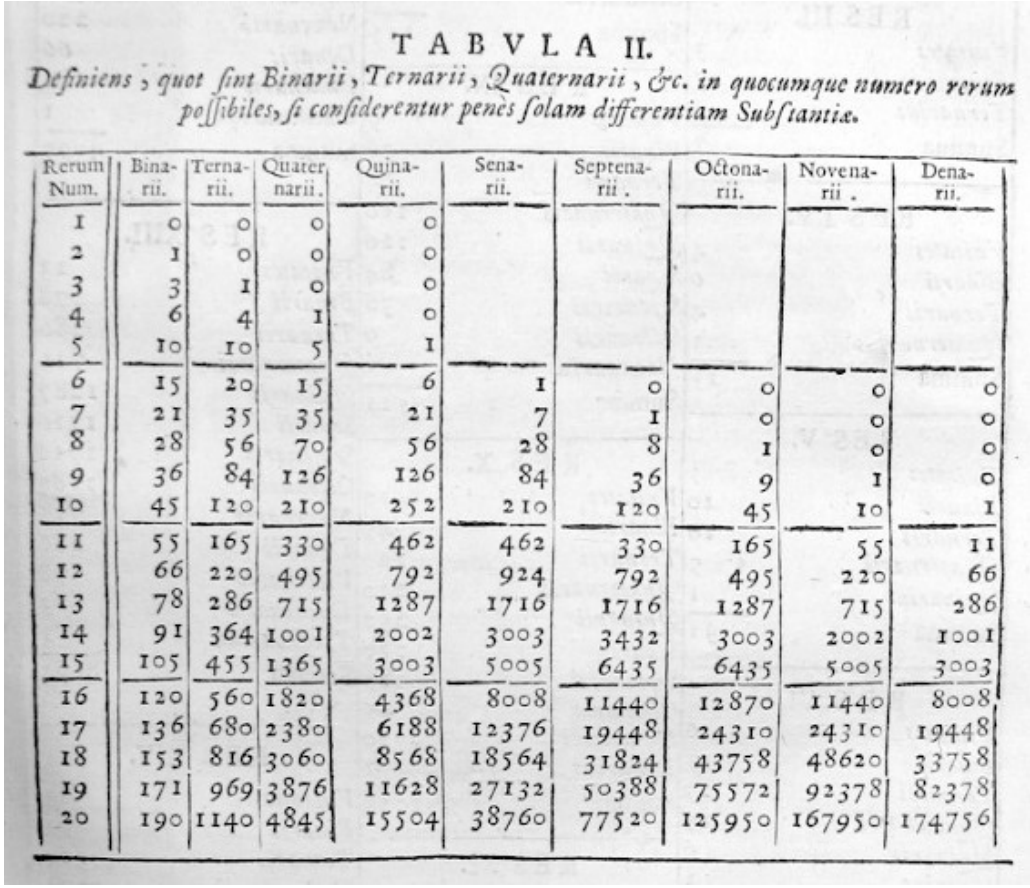
styl výkladu analogický předchozímu zkoumání jazyka
projevuje se nepochybná inspirace kabalou (např. permutace je matematickou formalizací a zobecněním *anagramu*)

pozornost je věnována určování počtu k-tic v závislosti na uplatněných diferencích
vždy podrobné odvození, v zásadě na principu indukce
výsledky uspořádány v tabulce
Caramuel formuluje jednoduchá pravidla, jak hodnoty v jednotlivých polích spolu souvisí a jak lze tabulku dále konstruovat
v této podobě i princip Pascalova trojúhelníka

Ukázka *anagramu*



Tabulka s počty kombinací



TABVLA II.

Definiens, quot sint Binarii, Ternarii, Quaternarii, &c. in quocumque numero rerum possibiles, si considerentur penès solam differentiam Substantiæ.

Rerum Num.	Bina-rii.	Terna-rii.	Quater-narii.	Quina-rii.	Sena-rii.	Septena-rii.	Octona-rii.	Novena-rii.	Dena-rii.
1	0	0	0	0					
2	1	0	0	0					
3	3	1	0	0					
4	6	4	1	0					
5	10	10	5	1					
6	15	20	15	6	1	0	0	0	0
7	21	35	35	21	7	1	0	0	0
8	28	56	70	56	28	8	1	0	0
9	36	84	126	126	84	36	9	1	0
10	45	120	210	252	210	120	45	10	1
11	55	165	330	462	462	330	165	55	11
12	66	220	495	792	924	792	495	220	66
13	78	286	715	1287	1716	1716	1287	715	286
14	91	364	1001	2002	3003	3432	3003	2002	1001
15	105	455	1365	3003	5005	6435	6435	5005	3003
16	120	560	1820	4368	8008	11440	12870	11440	8008
17	136	680	2380	6188	12376	19448	24310	24310	19448
18	153	816	3060	8568	18564	31824	43758	48620	33758
19	171	969	3876	11628	27132	50388	75572	92378	82378
20	190	1140	4845	15504	38760	77520	125950	167950	174756

Sv. Josef

Sv. Josef – detail

Sv. Jan Nepomucký

Sv. Jan Nepomucký – detail

inskripce

SanCto IoannI NepoMVCeno
CoronaeCzeChICae /
ReglnVrbIsTrVtnoVIeInsIgnI
proteCtorI

Děkuji vám za pozornost.