834. 6. *Цегелик Г.Г., Кудеравець Х.С. Апроксимація часткових сум узагальнених гармонічних рядів неперервними функціями // Вісн.Львів.у-ту. Сер.мех.-мат. 1995. Вип.42. С. 17-19.*

УДК 681.3

***В.С.Якушев, Д.А.Чепурний***

***НУ "Львівська політехніка", кафедра інформаційних систем та мереж***

# ПЕРЕТВОРЕННЯ Й ОПРАЦЮВАННЯ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ АЛГОРИТМУ КАНТОРА І ТЧП



**The method for number-theoretic transformations (NTT) with using residual class number system is presented. It is based on number representation of Cantor algorithm. The result is a computing complication and hardware cost reduction of NTT.**

Застосування алгоритму Кантора для перетворення і опрацювання інформаційних потоків вважається ефективним у випадку подальшого цифрового опрацювання сигналів (електричних) за допомогою апарату теоретико-числових перетворень, зокрема Китайської теореми про залишки (КТЗ) [1]. Алгоритм Кантора [2] дозволяє відображати вхідну аналогову величину в цифровому вигляді, який найприйнятніший для застосування КТЗ, тобто у вигляді залишків за кількома модулями. КТЗ підвищує швидкодію опрацювання інформації за рахунок здійснення обчислень паралельно і незалежно за кожним з модулів. Окрім того, сумісне застосування алгоритму Кантора і КТЗ підвищує швидкодію переходу від числового відображення в нормальному вигляді до системи залишків і навпаки, а також знижує складність цього переходу, що є одним з основних стримуючих факторів для застосування при обчисленні дійсних чисел у вигляді системи залишків [3]. Ця стаття є продовженням роботи [2].

Метою досліджень є зменшення обчислювальної складності та апаратурної вартості обчислення теоретико-числових перетворень (ТЧП) за рахунок використання відображення дійсних чисел швидкозбіжними рядами, а також отримання співвідношень, які дозволяють оцифровувати дані в необхідному для ТЧП вигляді на основі сучасних способів перетворення інформації, в тому числі аналого-цифрового перетворення.

Основними методами, що використовуються при цифровому опрацюванні сигналів, є згортка та гармонічний аналіз. Відомо, що згортку можна обчислювати за допомогою спектральних методів, але порівняно недавно стало відомо, що й гармонічний аналіз можна проводити, обчислюючи систему згорток.

Поява нових порівняно з швидким перетворенням Фур'є [1] алгоритмів, таких як алгоритми простих множників Томаса-Гуда, алгоритм Рейдера (зведення до циклічної згортки), алгоритм Тоома-Кука, алгоритм Винограда перетворення Фур'є та алгоритм простих множників, стала новим етапом у розвитку прикладного гармонічного аналізу. Усі згадані алгоритми стосувались кодування області визначення дискретних сигналів (відліків часу і простору) відповідно до КТЗ. Було досягнуте ефективне обчислення дискретного перетворення Фур'є (ДПФ) у вигляді системи коротких згорток [6].

Кодування області значення сигналів в деякому скінченному числовому або поліноміальному полі призвело до появи ТЧП, які забезпечують циклічну згортку та ДПФ. Методи цілочислової арифметики, які використовуються в ТЧП, дозволили отримати нові покращені алгоритми цих перетворень.

Значного підвищення ефективності ТЧП можна досягнути за рахунок застосування системи числення в залишкових класах (СЗК) [4], що базується на КТЗ. Застосування СЗК дає змогу виконувати арифметичні операції з великою швидкістю через відсутність переносів від розряду до розряду. У такій системі число $a$ відображається своїми залишками $a_i$ за сукупністю взаємно простих модулів $m_i$ [5]

$$a = \{a_1, a_2, ..., a_i\}$$

Тоді додавання та множення двох чисел $a$ та $b$ може виконуватись додаванням та множенням залишків $a_i$ та $b_i$ за кожним модулем $m_i$ незалежно один від одного. Тому залишкове відображення чисел дуже ефективне для виконання арифметичних операцій з великою швидкістю. Однак переваги обмежуються практичними труднощами в застосуванні ТЧП: складністю та вартістю переходу до залишків і відновлення результату.

Для усунення цих недоліків пропонується:

1. На етапі оцифровування даних використовувати для перетворення інформації алгоритми відображення дійсних чисел швидкозбіжними рядами (зокрема алгоритмом Кантора), які дозволяють подати вхідну аналогову величину в цифровому вигляді, найбільш прийнятному для застосування СЗК, тобто у вигляді залишків за сукупністю взаємно простих модулів — основ системи.

2. Використовувати алгоритм Кантора при відновленні результату за сукупністю залишків.

У першому випадку усувається необхідність обчислення залишків числа на етапі, що передує ТЧП, у другому — труднощі, пов'язані з відновленням результату, з одночасним зниженням складності і підвищенням швидкості відновлення.

Зміст пропонованого методу полягає в такому. Довільне дійсне число $\gamma$ відображається рядом Кантора. Нехай $m_1, m_2, m_3, ...$ — послідовність довільних цілих чисел, що визначається як $m_i \geq 2, i = 1, 2, 3, ...$. Позначимо $C_0$ найбільше ціле число, що не перевищує д.ч. $\gamma$. Із співвідношення для д.ч. $\gamma$: $\gamma = C_0 + \dfrac{\gamma_1}{m_1}$ визначимо д.ч. $\gamma_1$.

Оскільки $\gamma\ C_0 < 1$, то $0 \leq \gamma_1 < m_1$. Далі, за аналогією з попереднім припущенням, нехай

$C_1$ — найбільше ціле число, що не перевищує д.ч. $\gamma_1$, тоді д.ч. $\gamma_2$ визначимо із співвідношення для д.ч. $\gamma_1$: $\gamma_1 = C_1 + \dfrac{\gamma_2}{m_2}$, тобто $0 \le \gamma_2 < m_2$ і т.д.

Подібний процес можна записати у вигляді системи співвідношень

$$\left.\begin{aligned} \gamma_i &= C_i + \frac{\gamma_{i+1}}{m_{i+1}} \\ C_i &\le \gamma_i \\ 0 &\le \gamma_{i-1} < m_{i+1} \end{aligned}\right\} (i = 0, 1, 2, \ldots), \tag{1}$$

які дозволяють отримати відображення д.ч. $\gamma$ у вигляді ряду Кантора

$$\gamma_k = \gamma = C_0 + \sum_{i=1}^{n} \frac{C_i}{m_1 \cdot m_2 \cdot \ldots \cdot m_i} + \frac{\gamma_{n+1}}{m_1 \cdot m_2 \cdot \ldots \cdot m_{n+1}}, \tag{2}$$

при умові, що в (1) $\gamma_0 = \gamma$.

Максимальна абсолютна похибка наближення нескінченного ряду його кінцевим відрізком, тобто сумою цілої частини $C_0$ та $n$ ($n \not\longrightarrow \infty$) дробових членів визначається залишком ряду

$$\Delta_k = \frac{\gamma_{n+1}}{m_1 \cdot m_2 \cdot \ldots \cdot m_{n+1}} < \frac{1}{m_1 \cdot m_2 \cdot \ldots \cdot m_n} \le \frac{1}{2^n}.$$

Обмежившись $n$ першими членами ряду при умові $\gamma < 1$, отримаємо

$$\gamma = \sum_{i=1}^{n} \frac{C_i}{\prod\limits_{k=1}^{i} m_k}, \quad \gamma \le 1. \tag{3}$$

Позначимо $M = \prod\limits_{i=1}^{n} m_i$. Помноживши праву і ліву частини (3) на $M$, отримаємо

$$x = \gamma M = C_n + \sum_{i=1}^{n-1} \left( C_i \prod_{k=i+1}^{n} m_k \right). \tag{4}$$

З наведених вище співвідношень випливає, що будь-яке дійсне число $\gamma$ $(\gamma \le 1)$ може відображатись через розклад в ряд Кантора як ціле число $x$ $(x \le M)$ та може бути відновлене за відомими коефіцієнтами цього ряду $C_i$.

Відновлення числа за його залишками базується на КТЗ.

**Теорема.** Нехай $m_i$ $(i = 1, 2, .., n)$ — $n$ додатних попарно взаємно простих цілих, більших за одиницю $(m_1 \ge 2)$. Тоді система лінійних порівнянь

$$x \equiv r_i \bmod m_i, (i = 1, 2, ..., n) \tag{5}$$

має єдиний за модулем $M$ розв'язок, де $M = \prod_{i=1}^{n} m_i$

$$x = \sum_{i=1}^{n} \left(\frac{M}{m_i}\right) r_i T_i \bmod M, \;\; де \;\; \left(\frac{M}{m_i}\right) T_i \equiv 1 \bmod m_i . \qquad (6)$$

Знайдемо співвідношення, яке пов'язує відображення деякого цілого числа $x$ $(x \le M)$ рядом Кантора і відображення того самого числа сукупністю залишків, при умові, що $m_i$ — попарно взаємно прості додатні цілі числа, тотожні в обох відображеннях. Оскільки будь-яке додатне ціле число, що не перевищує $M$, має єдине, при заданих $m_i$ $(i = 1, 2, ..., n)$, відображення у вигляді ряду Кантора та у вигляді залишків, то, підставивши праву частину (4) в систему порівнянь (5), визначимо співвідношення, яке пов'язує залишки $r_i$ з коефіцієнтами $C_i$ ряду Кантора.

$$r_i = \left( C_n + \sum_{l=1}^{n-1} \left( C_l \prod_{k=l+1}^{n} m_k \right) \right) \bmod m_i \;, \;\; i = 1, 2, ..., n . \qquad (7)$$

Враховуючи, що при умові $l < i$

$\prod_{k=l+1}^{n} m_k \equiv 0 \bmod m_i, l = 1, 2, ..., n-1; i = 1, 2, ..., n,$ отримаємо

$$r_i = \left( C_n + \sum_{l=i}^{n-1} \left( C_l \prod_{k=l+1}^{n} m_k \right) \right) \bmod m_i \;, \;\; i = 1, 2, ..., n . \qquad (8)$$

Вимагаючи виконання умов

$$m_k \equiv 1 \bmod m_i, i = 1, 2, ..., n; k = i+1, i+2, ..., n, \qquad (9)$$

порівняння (8) можна записати у вигляді

$$r_i = \sum_{l=i}^{n} C_l \bmod m_i , \;\; i = 1, 2, ..., n . \qquad (10)$$

Проілюструємо викладене на прикладі.

**Приклад 1**. Нехай $m_1 = 2, m_2 = 3, m_3 = 7$. $M = m_1 m_2 m_3 = 42$.

Розкладемо в ряд Кантора число $x = 39$. Оскільки 39<42, то $C_0 = 0$.

$\frac{39}{42} \cdot 2 = \frac{78}{42} = 1\frac{36}{42}$, звідки $C_1 = 1$.

$\frac{36}{42} \cdot 3 = \frac{108}{42} = 2\frac{24}{42}$, звідки $C_2 = 2$.

$\frac{24}{42} \cdot 7 = \frac{168}{42} = 4$, звідки $C_3 = 4$.

Оскільки в даному випадку виконуються умови (9), то відповідно до (10) запишемо

$$r_1 = (C_1 + C_2 + C_3) \bmod 2 = (1+2+4) \bmod 2 = 1,$$
$$r_2 = (C_2 + C_3) \bmod 3 = (2+4) \bmod 3 = 0,$$
$$r_1 = C_3 = 4,$$

що збігається з безпосереднім обчисленням залишків числа 39 за модулями 2, 3, 7:

$$39 \bmod 2 = 1, 39 \bmod 3 = 0, 39 \bmod 7 = 4.$$

Проілюструємо з використанням того самого прикладу відновлення числа $x = 39$ за відомими залишками на основі КТЗ.

**Приклад 2.** Нехай $m_1 = 2, m_2 = 3, m_3 = 7. M = 42$.

$$x = 39, r_1 = 1, r_2 = 0, r_3 = 4,$$

співвідношення (6) запишемо у вигляді

$$x = \left( \frac{M}{m_1} r_1 T_1 + \frac{M}{m_2} r_2 T_2 + \frac{M}{m_3} r_3 T_3 \right) \bmod 42. \tag{11}$$

Визначимо $T_i$ з порівнянь (6) $\left( \frac{M}{m_i} T_i \right) \equiv 1 \bmod m_i$

$$\frac{M}{m_1} = 21, \frac{M}{m_2} = 14, \frac{M}{m_3} = 6, T_i = \left( \frac{M}{m_i} \right)^{-1} \bmod m_i,$$

$$T_1 = (21)^{-1} \bmod 2 = 1^{-1} \bmod 2 = 1,$$
$$T_2 = (14)^{-1} \bmod 3 = 2^{-1} \bmod 3 = 2,$$
$$T_3 = (6)^{-1} \bmod 7 = 6.$$

Тоді вираз (11) набуде вигляду

$$x = (21 r_1 + 28 r_2 + 36 r_3) \bmod 42. \tag{12}$$

Оскільки залишок $r_1$ набуває значень з множини (0, 1), $r_2$ з множини (0, 1, 2), а $r_3$ з множини (0, 1, 2, 3, 4, 5, 6), то при проведенні обчислень за формулою (12) обчислені значення $28r_2$ та $36r_3$ можуть перевищити значення модуля, що потребує виконання операції приведення за модулем $M = 42$, окрім того, на етапі підсумовування проміжний результат може також перевищити цей модуль. У прикладі 2:

$$(21 r_1 + 28 r_2 + 36 r_3) \bmod 42 = (21 \cdot 1 + 28 \cdot 0 + 36 \cdot 4) \bmod 42 =$$
$$(21 + 144) \bmod 42 = 21 + 144 \bmod 42 = 21 + 18 = 39 \bmod 42.$$

Із зазначеного випливає, що обчислення за формулою (12) потребує застосування спеціальних множильних та підсумовуючих пристроїв, здатних виконувати множення та додавання за складним модулем $M$. Це створює додаткові труднощі навіть в тому випадку, коли числа $m_i, i = 2, ..., n$ вибрані числа Мерсена вигляду $2^p - 1$. Внаслідок цього збільшуються часові та апаратні витрати.

Відображення рядом Кантора можна використати для відновлення чисел за коефіцієнтами відповідного ряду $C_i$, обчисливши їх попередньо за відомими залишками $r_i$. У такому разі обчислення за формулою (4) стають менш складними, ніж за формулою (6). Покажемо це на прикладі для $n = 3$.

**Приклад 3.** $m_1 = 2, m_2 = 3, m_3 = 7. M = 42$.

Запишемо вираз (4) у вигляді

$$x = m_2 m_3 C_1 + m_3 C_2 + C_3,$$

підставивши числові значення $m_1, m_2, m_3$, отримаємо

$$x = 21C_1 + 7C_2 + C_3. \tag{13}$$

Оскільки $C_1, C_2, C_3$ набувають значень з тієї самої множини, що й $r_1, r_2, r_3$ відповідно, то проміжні результати, обчислені за формулою (13), на жодному з етапів, зокрема на останньому етапі підсумовування, не перевищують модуля та відсутня одна з операцій множення. Окрім того, на етапі множення може бути застосований зрізаний матричний множник (наприклад: значення $7\,C_2$ ніколи не перевищує 14). Це значно зменшує складність обчислень порівняно з виразом (12).

Для знаходження коефіцієнтів ряду Кантора за відомими залишками $r_i$ необхідно розв'язати систему лінійних порівнянь (8) відносно $C_i$.

Знайдемо цей розв'язок для $n = 3$.

Введемо позначення $a \bmod b \stackrel{def}{=} \langle a \rangle_b$. Тоді для знаходження $C_i$, якщо $n = 3$, необхідно розв'язати систему лінійних порівнянь

$$\begin{cases} \langle m_2 m_3 C_1 + m_3 C_2 + C_3 \rangle_{m_1} = r_1 \\ \langle m_3 C_2 + C_3 \rangle_{m_2} = r_2 \\ C_3 = r_3. \end{cases} \tag{14}$$

Звідки

$$\begin{cases} C_3 = r_3 \\ C_2 = \left\langle m_3^{-1} (r_2 - r_3) \right\rangle_{m_2} \\ C_1 = \left\langle (m_2 m_3)^{-1} \left( r_1 - r_3 - m_3 \left\langle m_3^{-1} (r_2 - r_3) \right\rangle_{m_2} \right) \right\rangle_{m_1}. \end{cases} \tag{15}$$

Якщо виконано умови (9), розв'язок (14) можна записати у вигляді

$$\begin{cases} C_3 = r_3 \\ C_2 = \left\langle \left( r_2 - r_3 \right) \right\rangle_{m_2} \\ C_1 = \left\langle r_1 - r_3 - \left\langle \left( r_2 - r_3 \right) \right\rangle_{m_2} \right\rangle_{m_1}. \end{cases} \quad (16)$$

**Приклад 4.** $m_1 = 2, m_2 = 3, m_3 = 7. M = 42$.

$$x = 39, r_1 = \langle 39 \rangle_2 = 1, r_2 = \langle 39 \rangle_3 = 0, r_3 = \langle 39 \rangle_7 = 4.$$

$$C_3 = r_3 = 4,$$

$$C_2 = \left\langle \left( r_2 - r_3 \right) \right\rangle_{m_2} = \langle -4 \rangle_3 = 2,$$

$$C_1 = \langle 1 - 4 - C_2 \rangle_{m_1} = \langle 1 - 4 - 2 \rangle_2 = 1.$$

Отримані значення $C_1, C_2, C_3$ збігаються з коефіцієнтами розкладу числа 39 у прикладі 1. Обчислення для визначення $C_i$ тривіальні та здійснюються за модулями $m_i$ відповідно, що дає можливість виконати їх на обчислювальній структурі, яка використовувалась до операції відновлення.

Наведемо приклади можливих обчислювальних структур для класичного, із застосуванням КТЗ, та запропонованого варіантів, включно з аналого-цифровим перетворенням (рис. 1, 2).

Слід зазначити, що реалізація помножувача та суматора за $\mathrm{mod}\, M \left( M = \prod_{i=1}^{n} m_i \right)$ (рис.1) далеко не тривіальна, оскільки потребує проведення складних обчислень за складним модулем $M$. Через вказані причини, а також із зіставлення відомої та запропонованої блок-схем розв'язування задачі в СЗК, слід очікувати від реалізації останньої зниження апаратурних витрат та підвищення швидкодії.

У ході проведених досліджень встановлено також, що доцільно застосувати пропонований метод для розв'язування задач за допомогою поліноміальних перетворень, а саме для обчислення згортки. Це зумовлено тим, що в ряд Кантора розкладаються не тільки цілі числа, але й поліноми.

Метою подальших досліджень є побудова ефективних алгоритмів цифрового опрацювання сигналів у скінченних числових та поліноміальних полях на основі запропонованого методу, а також дослідження інших СЗК (наприклад, в комплексній області) та рядів для відображення цілих чисел та поліномів.

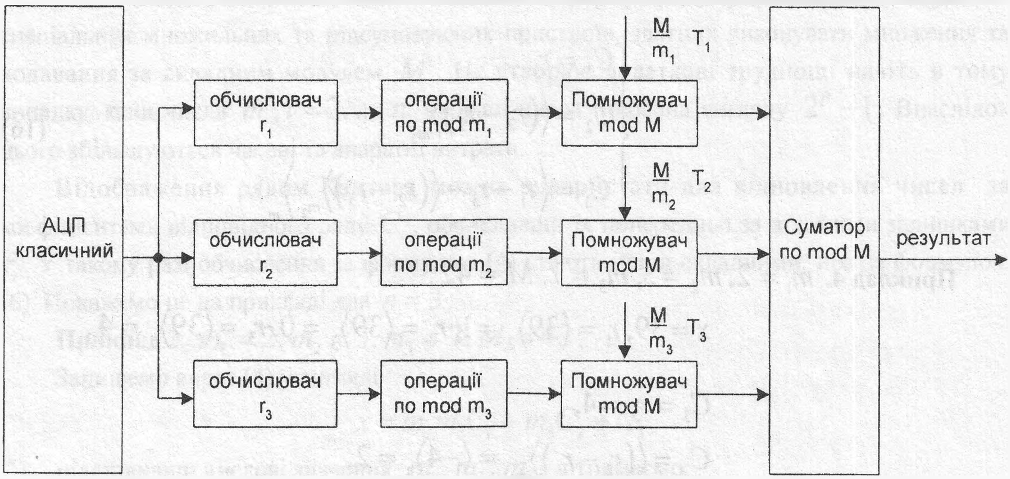


**Рис. 1.** Класична блок-схема розв'язування задачі із застосуванням СЗК

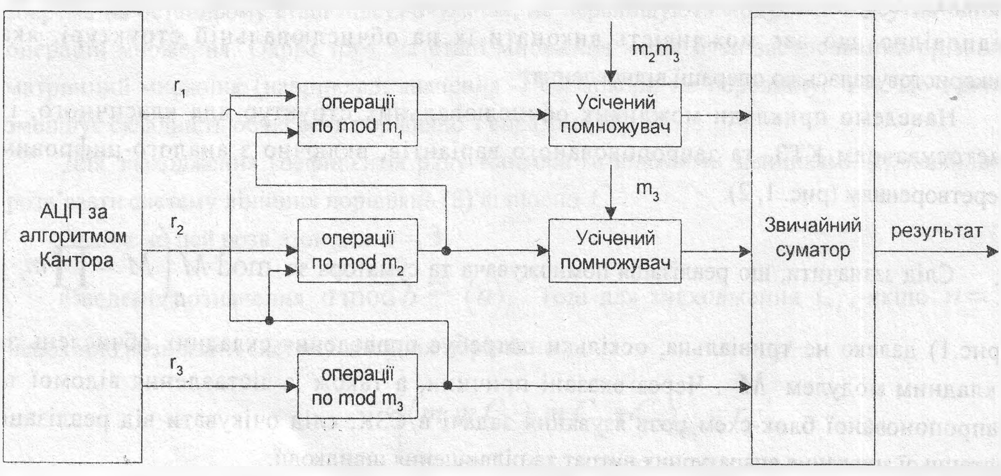


**Рис. 2.** Запропонована блок-схема розв'язування задачі із
застосуванням СЗК і відображення д.ч. за алгоритмом Кантора

*1. А.Ахо, Дж.Хопкрофт, Дж.Ульман Построение и анализ вычислительных алгоритмов. М.,1979. 2. Якушев В.С. Використання активних алгоритмів перетворення і опрацювання інформації в інформаційних технологіях // Вісник ДУ "Львівська політехніка". 1999. № 383. С. 242-260. 3. Якушев В.С., Сварчевский Г.С. Методы получения дискретизированных данных для сверхточных алгоритмов реконструкции, основанные на использовании аппарата быстросходящихся рядов // Тез. докл. III*

*Всесоюзного симпозиума по вычислительной томографии. К,, 1987. 4. Торгашев В.А. Система остаточных класов и надежность ЦВМ. М., 1973. 5. Аршинов М.Н. Коды математика. М., 1983. 6. Блейхут Г. Быстрые алгоритмы цифровой обработки сигналов. М., 1989.*

УДК 681.3

***Ю.В.Яцишин, Н.Б.Шаховська***

***НУ "Львівська політехніка", кафедра інформаційних систем та мереж***

# МОДЕЛЬ УПРАВЛІННЯ МІСТОМ НА ОСНОВІ ТЕРМОДИНАМІЧНИХ ЗАКОНІВ



**Authors of given article offer to represent a macroeconomic town model in appearance of thermodynamic system. A Basic idea is in use of thermodynamics laws for modeling of economic processes. For her realization was seen out comparative description of basic parameters of economic and thermodynamic systems and defined the joint lines in their conduct. A Program, which can be created on use base of thermodynamic laws, will allow to model a town economy state in dependence on given alternatives and development ideas. In given article counted the basic demands to such model and use variants of results found by it.**

Управління — одна з найважливіших функцій держави. Управління економічною системою — невід'ємна частина процесу управління загалом. Економіка — відносини людей у процесі досягнення цілей при обмежених можливостях. Оскільки людей і цілей багато, а обмеження, які виникають, дуже різноманітні за якістю, то економіку можна вважати дуже складною системою, яку важко прогнозувати та моделювати.

Поняття економічної цілі часто буває дуже розмитим. Люди хочуть одного, а одержують інше, видозмінюють свої цілі, а іноді відмовляються від них, звертаючись до інших. Більше того, якщо навіть у поведінці учасника економічних відносин виявляється домінанта цілей, то цілком можливо, що вона міститиме іншу, приховану і навіть неусвідомлену ціль.

Класифікація цілей дуже важлива для адекватного опису моделі управління та економіки зокрема, і не настільки важливо те, щоб кожна ціль розумілася правильно, як те, щоб сукупність усіх цілей являла собою збалансовану систему людських інтересів. Тоді ми одержимо деяку модель економіки, у якій невеличка кількість показників економічної діяльності зрозумілим чином пов'язане з інтересами людей. Таку модель називають макроекономічною, і вона буде являти собою лінійний простір всіх економічних ідей.