Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 6 August 2024

Case Number: T 0323/21 - 3.4.01

Application Number: 15849344.5

Publication Number: 3206201

IPC: G09C1/00, G06F9/44, H04L9/28

Language of the proceedings: EN

Title of invention:
NON-DECREASING SEQUENCE DETERMINING DEVICE, NON-DECREASING SEQUENCE DETERMINING METHOD, AND PROGRAM

Applicant:
Nippon Telegraph and Telephone Corporation

Headword:
Non-decreasing sequence determining device / Nippon Telegraph and Telephone Corp.

Relevant legal provisions:
EPC Art. 52(1), 56

Keyword:
Patentable invention - technical and non-technical features - mathematical method

Decisions cited:
T 0154/04

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0

Case Number: T 0323/21 - 3.4.01

D E C I S I O N
of Technical Board of Appeal 3.4.01
of 6 August 2024

Appellant: (Applicant)	Nippon Telegraph and Telephone Corporation 5-1, Otemachi 1-chome, Chiyoda-ku, Tokyo 100-8116 (JP)
Representative:	MERH-IP Matias Erny Reichl Hoffmann Patentanwälte PartG mbB Paul-Heyse-Strasse 29 80336 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 13 November 2020 refusing European patent application No. 15849344.5 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	P. Scriven
Members:	P. Fontenay
	D. Rogers

Summary of Facts and Submissions

I. The appeal is of the Examining Division's decision, of the Examining Division of the European Patent Office refusing the patent application.

II. The contested decision was taken by reference to two earlier communications of the Examining Division. Only the second of those communications referred to the claims on file, that is to the claims filed on 6 August 2020.

III. The Examining Division held that the claimed subject-matter was not sufficiently clear (Article 84 EPC), considering the definition of index j in the identification of vectors b_{ij} and t_{jk}. Moreover, when determining whether a nondecreasing sequence existed within the indicated number of merges, the skilled person was left in doubt as to how to select the various indices, i, j, and k. It was also doubted that the advantage of determining the existence of a nondecreasing sequence within a number of rounds corresponding to $ceil(log_2(m))$ was achievable (Article 83 EPC).

IV. The first of the communications to which the refusal referred related to claims filed earlier in the proceedings. It is not clear how the objections raised in this earlier communication apply to the last version of the claims.

V. In the notice of appeal and the statement of grounds, the appellant requested the setting aside of the impugned decision and the grant of a patent on the basis of the claims underlying the refusal.

VI. The view that the claim did not allow identification of appropriate triplets *(i, j, k)* that achieved the intended purpose of determining whether a nondecreasing sequence existed, was contested. The claimed approach relied on a typical iterative process of divide and conquer, in view of the aim of the invention to find, for a given value of m, the vector $t_{0,m}$ required to determine the existence of such a sequence.

VII. In the proprietor's view, the argument that the claimed subject-matter did not limit the number of merges to $ceil(log_2(m))$ rounds was based on a misunderstanding regarding the concept of the number of rounds: in the field of the invention, processes that could be executed in parallel were considered to be performed within one round.

VIII. In a communication under Article 15 RPBA, the appellant was informed of the Board's preliminary opinion that the features of claim 1 were sufficiently understandable (Article 84 EPC) for the skilled person to make sense of the claim and determine the list of triplets *(i, j, k)* that provides the sought information regarding the existence of a nondecreasing sequence. Contrary to the assumption made by the Examining Division (letter of 15 November 2020), the skilled person would have recognised that an arbitrary selection of triplets *(i, j, k)*, with *i*, *j*, and *k*

fulfilling the recited conditions, would not have been sufficient to achieve the claimed purpose of determining the existence of nondecreasing sequences. It was realistic to assume that the skilled person would have operated differently from this arbitrary approach, and elaborated, on the basis of common general knowledge and the recited criteria, a strategy that led to the desired result. Eventually, the skilled person would have defined a list of triplets as set out on page 3, third paragraph, of the statement of grounds. It was, in particular, assumed that the skilled person working in the technical field of the invention was well versed in mathematical issues and would have known how to proceed to achieve the recited result (Article 83 EPC).

IX. It was further observed that independent claims 1 and 2 as to a device, and 3 and 4 as to the corresponding methods, did not enter into any of the categories listed in Rule 43(2) EPC justifying the existence of a plurality of independent claims in one category. The presence of two claims per category did not appear to be allowable.

X. In reply to the Board's communication, the appellant filed a new main request and new auxiliary requests 1 and 2. All new requests included a single device claim, a single method claim, and a claim directed to a program for causing a computer to function as the device of claim 1.

XI. Oral proceedings before the Board took place in presence of the appellant. In the course of them, the

debate focused on the questions of whether the description was sufficient to allow the skilled person to carry out the claimed invention and on the technicality of the claimed subject-matter.

XII. Claim 1 of the main request reads:

> *A nondecreasing sequence determining device (2), wherein m is an integer equal to or larger than 2;*
> *the nondecreasing sequence determining device (2) comprising:*
> *a sorting part (10) taking inputs of m sets P_0, ..., P_{m-1} and sorting elements of a set P_i in ascending order for i = 0, ..., m-1 to generate a vector $t_{i,i+1}$ and a vector $b_{i,i+1}$,*
> ***characterized in that** the nondecreasing sequence determining device (2) further comprises:*
> *a concealing part (40) generating an encrypted text <$t'_{i,i+1}$> in which a vector $t'_{i,i+1}$ is concealed and generating an encrypted text <$b'_{i,i+1}$> in which a vector $b'_{i,i+1}$ is concealed, wherein, in the vector $t'_{i,i+1}$, $t'_{i,i+1}[k]=1$ is set if λ that satisfies $t_{i,i+1}[\lambda]k$ exists for k = 0, ..., n-1 and λ=0,..., m-1, otherwise, $t'_{i,i+1}[k]=0$ is set, and in the vector $b'_{i,i+1}$, $b'_{i,i+1}[k]=1$ is set if λ that satisfies $b_{i,i+1}[\lambda]=k$ exists, otherwise $b'_{i,i+1}[k]=0$ is set, where each of elements of the sets P_0, ..., P_{M-1} is greater than 0 or equal to 0 and less than n;*

a merging part (50) merging secret texts $\langle t'_{0,1}\rangle$, ..., $\langle t'_{m-1,m}\rangle$ to generate a secret text $\langle t'_{0,m}\rangle$ and merging secret texts $\langle b'_{0,1}\rangle$, ..., $\langle b'_{m-1,m}\rangle$ to generate a secret text $\langle b'_{0,m}\rangle$ by repeating a process of merging secret texts $(\langle t'_{i,j}\rangle, \langle b'_{i,j}\rangle)$ and $(\langle t'_{j,k}\rangle, \langle b'_{j,k}\rangle)$ that satisfy $0\leq i<j<k\leq m$ to generate a secret text $(\langle t'_{i,k}\rangle, \langle b'_{i,k}\rangle$; and

a determining part (60) calculating $\langle t'_{0,m}[O]\rangle \vee \langle t'_{0,m}[1]\rangle \vee \ldots \vee \langle t'_{0,m}[m-1]\rangle$ by using the secret text $\langle t'_{0,m}\rangle$ and outputting the result of the calculation as the result of determination;

wherein the merging part (50) comprises:

a first stable-sorting part (51) alternately arranging elements of secret texts $\langle b'_{i,j}\rangle$ and $\langle t'_{j,k}\rangle$ to generate a secret text $\langle a\rangle$ and stable-sorting a secret text $(\langle (0,1)^n\rangle, \langle a\rangle, \langle (0, \ldots, 2n-1)\rangle)$ by using $\neg\langle a\rangle$ as a key to generate a secret text $(\langle f'\rangle, \langle a'\rangle, \langle p\rangle)$;

a first key-reveal-sorting part (52) calculating $\langle a'[h]\rangle \times (\neg\langle f'[h]\rangle \times \langle f'[h+1]\rangle + \langle f'[h]\rangle \times \neg\langle f'[h-1]\rangle)$ for $h = 0, \ldots, 2n-1$ to generate a secret text $\langle m\rangle$ and key-reveal sorting the secret text $\langle m\rangle$ by using a secret text $\langle p\rangle$ to generate a secret text $\langle m'\rangle$;

a second stable-sorting part (53) alternately breaking down elements of the secret text $\langle m'\rangle$ to generate secret texts $\langle m_0\rangle$ and $\langle m_1\rangle$, stably sorting $(\langle t'_{i,j}\rangle, \langle (0, \ldots, n-1)\rangle)$ by using $\neg\langle t'_{i,j}\rangle$ as a key to generate a secret text $(\langle t''_0\rangle, \langle p_0\rangle)$,

stably sorting the secret text <m_0> by using ¬<$b'_{i,j}$> as a key to generate a secret text <m''_0>, stably sorting (<$b'_{j,k}$>, <(0, ..., n-1)>) by using ¬<$b'_{j,k}$> as a key to generate a secret text (<b''_1>, <p_1>), and stably sorting the secret text <m_1> by using ¬<$t'_{j,k}$> as a key to generate a secret text <m''_1>; and
a second key-reveal-sorting part (54) generating a secret text <t"> that is the product of a secret text <t''_0> and a secret text <m''_0>, and a secret text <b"> that is the product of a secret text <b''_1> and a secret text <m''_1>, key-reveal sorting the secret text <t"> by using a secret text <p_0> as a key to generate a secret text <$t'_{i,k}$>, and key-reveal sorting the secret text <b"> by using a secret text <p_1> as a key to generate a secret text <$b'_{i,k}$>, where $(0, 1)^n$ is a vector being composed of 0s and 1s and having a length of 2n and ¬• denotes the negation of •.

XIII. Claim 1 according to first auxiliary request differs in that it include additional features regarding the "merging part (50)". Concretely, it contains the additional limitation:

[... to generate a secret text <$b'_{i,k}$>,] wherein the merging part (50) selects a combination of integers i, j, and k for each merging process, wherein for each combination, j is an integer satisfying 0 < j < m except integers already selected as j

for any previous merging process, i is an integer satisfying 0 ≤ i < j except integers already selected as j for any previous merging process, k is an integer satisfying j < k ≤ m except integers already selected as j for any previous merging process, and
i, j, and k satisfy the following formula:

$$j = \left\lfloor \frac{i+k}{2} \right\rfloor,$$

[where $(0,1)^n$....]

XIV. Claim 1 according to second auxiliary request corresponds to claims 1 according to first auxiliary request, with the only difference that "m is *an integer equal to or larger than 3*".

Reasons for the Decision

Background of the invention

1. The invention relates to an applied cipher technique and, in particular, to a method for determining whether a nondecreasing sequence exists, without revealing input data (paragraph [0001] of the published application).

2. There is a method, known from the prior art, called secure computation, for computing encrypted results from encrypted data without decrypting any of the encrypted data. Encryption is performed that

distributes pieces of a numerical value among a plurality of secure computers which cooperate to perform a computation in such a manner that the result is distributed among the secure computers without reconstructing the numerical value, that is, with the result and the original value being kept encrypted (paragraph [0002]).

3. According to a known method of pattern matching for character sequences on secure computation, this is accomplished by evaluating a non-deterministic finite pattern sequence, character by character, in an input text.

4. The process for determining whether a text matches a pattern after positions of partial character strings in the pattern have been identified can be abstracted to the problem of determining whether a non-decreasing sequence can be created, by selecting elements one by one, from each set of a sequence of sets. The invention is thus about determining whether such a non-decreasing sequence can be identified (paragraph [0006]). It seeks to perform pattern matching in a way that is compatible with encryption.

5. The technique according to the present invention determines, in $O(log(m))$ rounds, whether or not a nondecreasing sequence exists, by selecting elements one by one from each of m sets (paragraph [0008]). The device and method according to the invention seek efficiently to determine whether such a nondecreasing exists, thus enabling efficient pattern matching for texts.

Inventive step - technicality

6. The device of claim 1 according to the main request consists of a combination of functional units that cooperate to assess whether a nondecreasing sequence can be created from a sequence of sets of numbers. This is achieved by selecting elements, one by one from each set in the sequence. The claim does not contain any reference to any concrete use of the result. The various functional units of the device are defined by their mathematical roles in the determination of whether or not there is a nondecreasing sequence.

7. The claimed invention is a device. It therefore has technical character, as required by Article 52(1) EPC.

8. As recalled in decision T 154/04, *Estimating sales activity / DUNS LICENSING ASSOCIATES*, OJ EPO 2008, 46, inventive step (and even novelty) can be based only on technical features. "Non-technical features, to the extent that they do not interact with the technical subject matter of the claim for solving a technical problem, i.e. non-technical features 'as such', do not provide a technical contribution to the prior art and are thus ignored in assessing novelty and inventive step." Moreover, "[f]or the purpose of the problem-and-solution approach, the problem must be a technical problem which the skilled person in the particular technical field might be asked to solve at the relevant priority date" (cf. T 154/04, OJ 2008, 46).

9. This implies that the mathematical functionalities defined in claim 1, to the extent that they do not interact with technical features to produce a technical effect, cannot justify the existence of an inventive

step.

10. The technical nature of the claimed subject-matter is limited to the existence of the software code running on the claimed device.

11. In the absence, in claim 1, of reference to any concrete technical use or any physical entity required by the claimed device to carry out said process, no technical contribution resulting from the various mathematical operations running on the device can be identified.

12. The algorithm underlying the claimed device is exclusively of a mathematical nature. It is without any interaction with the device on which it operates. The technicality of the claimed device lies only in its materiality. Concretely, its technicality is limited to the combination of software code with the associated processing unit. The claimed device with its program code implements a purely mathematical method deprived, in its generality, of any technical purpose.

13. The applicant contested this view and underlined that the recited device and method were used for determining whether a text matched a pattern as in paragraph [0005] of the published application. They further stressed that the disclosed approach had the advantage of allowing a large number of merges to be carried out in parallel, thus reducing the number of rounds to achieve a result.

14. The applicant's arguments did not persuade the Board.

15. Independent claim 1 does not contain any concrete reference to a use of the claimed device and method.

Therefore, independently of the fact that text matching is not technical in itself, no technical contribution can be derived from any specific use of the claimed invention if it cannot be derived, explicitly or implicitly, from the claimed subject-matter.

16. While it is acknowledged that the reduction of the number of rounds to obtain a result can define an advantage over similar approaches, it is noted, in the absence in the claims of indications regarding the strategy to be followed by appropriately selecting the various indices, *i*, *j*, and *k*, that the limitation regarding the reduced number of merges cannot be derived from the present wording.

17. More fundamentally, the effect put forward by the applicant is also not sufficient to confer technical character to a method which is mathematical by nature. In the absence of interaction with the device on which the algorithm is to be run, the recited method does not add to its technical character.

18. Hence, the subject-matter of claim 1 of the main request does not define a technical solution to a technical problem. Hence, it is not inventive.

19. Claim 1 of auxiliary request 1 includes additional features regarding the "merging part (50)", which have the effect of limiting the number of merges needed to reach a result. However, the reason developed above regarding the absence of technicality of the claimed method, also apply to this claim. The amendments are not sufficient to define a technical solution to a technical problem. Hence these claims are not inventive.

20. The objections raised above with regard to the main request are not affected by the statement that m is an integer equal to or larger than 3, instead of 2 in the previous requests. The objections apply *mutatis mutandis* to the claims of the second auxiliary request which are thus not inventive.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

D. Meyfarth P. Scriven

Decision electronically authenticated