



Jack van Lint (1932–2004): A survey of his scientific work

Bram van Asch^a, Aart Blokhuis^a, Henk Hollmann^b, William Kantor^c,
Henk van Tilborg^a

^a *Department of Mathematics and Computing Science, Eindhoven University of Technology, PO Box 513,
5600 MB Eindhoven, The Netherlands*

^b *Philips Research Laboratories, High Tech Campus HTC-36, room WO-p-78 (M/S 02)5656 AE Eindhoven,
The Netherlands*

^c *Department of Mathematics, University of Oregon, Eugene, OR 97403-1222, USA*

Received 1 January 2006

Available online 13 June 2006

Abstract

When Jack van Lint was appointed as full professor at the Eindhoven University of Technology at the age of 26 he combined a PhD in number theory with a very open scientific mind. It took a sabbatical visit to Bell Laboratories in 1966 to make him understand that a new and fascinating field of applied mathematics was emerging: discrete mathematics. It fascinated and inspired him for the rest of his life. When he passed away on September 28, 2004, he left behind a legacy of 18 books and 177 articles, covering many aspects of coding theory, combinatorics, and finite geometry.

van Lint was also a strong international advocate of the role that discrete mathematics ought to play in modern applied mathematics curricula. Quite a few departments sought his advice. Years later, four different universities showed their appreciation by awarding him an honorary degree.

This overview is an homage to van Lint's academic achievements and can serve as an introduction to his work for younger generations.

© 2006 Elsevier Inc. All rights reserved.

Keywords: Coding theory; Combinatorial designs; Geometry; Number theory; Mathematical education

E-mail address: h.c.a.v.tilborg@tue.nl (H. van Tilborg).

1. The coding theorist

1.1. Perfect codes

In 1967 we see van Lint's first (joint) publication [20] on a coding theory related problem: the *football pool problem*. The question here is how many columns of outcomes one has to fill in for n soccer matches (a team wins, loses, or there is a draw), in order to be sure that at least one column will have at least $n - 1$ outcomes correctly. This problem can be reformulated as a *covering problem*: how many spheres of radius 1 around words in $\{0, 1\}^n$ are needed to cover $\{0, 1\}^n$ entirely? For $n = (3^m - 1)/(3 - 1)$, $m \geq 2$, the solution is given by the ternary *Hamming code*: 3^{n-m} columns need to be filled in. For other values of n the exact answer is a difficult open problem. The answer for $n = 5$ is 27, see [20]. van Lint realized that this is an ideal problem for the combinatorial search technique of simulated annealing. In [123], this technique is used to derive upper bounds when $n = 6, 7, 8$. These upper bounds are 73, 186, respectively 486. A survey of some results on covering codes in general and on the football pool problem in particular up to 1987 is given in [122].

A little later, van Lint became intrigued by *perfect codes*. These codes have the property that spheres with radius e around the codewords form a partitioning of $GF(q)^n$. In other words, these spheres are disjoint and cover the space. Known examples are the whole space ($e = 0$), the (trivial) binary repetition codes of odd length ($n = 2e + 1$), the Hamming codes ($e = 1$, $n = (q^m - 1)/(q - 1)$) and the two Golay codes: [23,12,7] over $GF(2)$ and [11,6,5] over $GF(3)$. These codes satisfy Hamming's bound: the number of codewords times the volume of a sphere with radius e must equal q^n . The non-trivial perfect codes are interesting from a mathematical point of view too because they have highly transitive automorphism groups and generate strong t -designs. Soon, his results attracted international attention, even though they were all of a negative kind. He studied more carefully Lloyd's theorem, which states that the characteristic polynomial of a code, called Lloyd's polynomial in the case of perfect codes, should only have integer zeroes in the interval $[1, n]$. He showed in [26] that no perfect, 2-error-correcting codes exist for $q \geq 5$ and that apart from the binary Golay code no other perfect, 3-error-correcting codes exists. At the IEEE Information Theory symposium in Noordwijk he presented these results in a plenary session [25]. In [29], we see an overview of all known results concerning perfect codes (often a computer was used to exclude cases) and it was shown with the same techniques that non-trivial, binary, 4-error-correcting, perfect codes do not exist. In [30], he showed that for any $e \geq 4$, there are only a finite number of values of n and q for which a perfect codes can exist and these values can be checked/excluded by computer search. He did this for $e = 4$ and showed that no non-trivial, 4-error-correcting, perfect code exists. He also showed that in general for $e > 3$ one needs that $p > e$, where q is a power of p . In [43] the results above are combined with that of [Ti73], where $p \leq e$ is derived as a necessary condition and concluded that for $e \geq 3$ the binary Golay code is the only perfect code. [49] is a nice survey of all these results; also some possible generalizations are discussed, like *nearly-perfect codes*. A more elementary proof of Lloyd's theorem is given in [68].

More than twenty years later, perfect codes again attracted his interest, but now with the additional requirement that the words are of constant-weight. Lloyd's theorem no longer holds and the techniques used are of a combinatorial nature. In [160], the authors observed that shortening a perfect, ternary, single error-correcting, constant weight code again gives such a code, which implies that repeated shortening results in a perfect binary code. They explicitly constructed an infinite family of ternary, perfect, single error-correcting codes of length $n = 2^l$, $l \geq 3$, and

constant weight $w = n - 1$ and showed that for other parameters no ternary, perfect, single error-correcting, constant weight codes exist. In [167], the authors tried to generalize the above ideas to field size $q = t + 1$ with $t = 2^k$. The shortening still works and a construction is given for $w = q = t + 1$ and $n = w + 1$.

1.2. Further results in coding theory

In 1973, van Lint became interested in the potential of *concatenated codes* [37], as codes that asymptotically have interesting parameters, meaning that the information rate and the relative error-correcting capability (# errors per codeword) stay positive when their length tends to infinity. In 1982 *algebraic-geometry codes* were introduced. They form a generalization of Goppa codes and exceed the Gilbert–Varshamov bound. In [113] it is shown that algebraic-geometry codes can also be described as a generalization of Reed–Solomon codes. The character of this paper as well as of [125] is more tutorial of nature. The papers [128,157,158] are excellent introductions to algebraic-geometry codes. In [149], the authors used the *order* function to construct a class of error-correcting “evaluation” codes, containing one-point algebraic-geometry codes and generalized Reed–Muller codes, without making use of the heavy machinery of algebraic-geometry.

The *Nadler code* is a binary, non-linear code of length 12 and minimum distance 5, containing 32 codewords. The original description shows no structure, but later a method was found to obtain it from the binary Golay code. In [34], a direct construction can be found that also allows a natural way to find the automorphism group of this code: the even part of $S_3 \times S_4$ (which is a transitive group of order 72).

In [39], the authors used the ternary Golay code to construct a very particular *strongly regular graph* on 243 points: two adjacent vertices are in exactly one triangle, while two non-adjacent vertices are in exactly one quadrangle.

Before [72,80], *quadratic residue* codes of length p were already generalized in the literature to length p^m , but van Lint felt that the existing descriptions were too obscure or too abstract. The group algebra approach allowed an easier description and a simpler way to determine automorphisms of these codes or to derive the square-root bound on the minimum distance.

Number theory returns in [74], where an introduction is given to the connections between coding theory, sphere-packings, lattices, modular functions and θ -functions. It includes the construction of two famous lattices from coding theory: $\Lambda(H_8)$ from the binary extended Hamming code of length 8 and Λ_{24} from the binary Golay code.

Genetic local search algorithms form a particular approach to combinatorial optimization problems. They make use of a parallel between these problems and some biological evolution processes. This technique was applied in [135] to get better lower bounds on $A_3(n, 3)$, the size of the largest ternary code of length n with minimum distance 3. Also some constructions of such codes were given.

Results on Kerdoock and Preparata codes [96,97] are discussed in Chapter 4. In [92] one can find an introduction to coding theory, Reed–Muller codes and Kerdoock codes.

The paper [110] by van Lint and Wilson represented a breakthrough in the analysis of the minimum weight of cyclic codes based on their zeros only. Here, they developed several new methods such as the *AB*-method providing, for example, a simple proof of the Roos bound, and a powerful new approach called shifting (the corresponding bound is usually referred to as the shift-bound). These methods (occasionally in combination with the weight-divisibility theorem

of McEliece [McE72]) are powerful enough to determine the true minimum distance of all binary cyclic codes of length less than 63, with only two exceptions.

van Lint continued to contribute to these topics with several of his master's students. In [134], van Lint and van Eupen used these methods to determine the minimum weight of most of the ternary cyclic codes of length less than 40, and many of those with a length between 41 and 50. To handle some of these cases, they developed several new methods based on analysis of subcodes, contractions, or other particular codes constructed from the code under investigation.

Earlier, in [131] van Lint and de Rooij investigated the minimum distance of the two binary cyclic codes of length 65 for which the methods from [110] fail. They show that the desired result can be obtained by using Jensen's method with some improvements. Their basic idea is to show that for certain concatenated codes not all the non-zero symbols of a word of minimum weight from the outer code are mapped to words of minimum weight in the inner code.

One of the results from [110] states that the minimum distance of a binary cyclic code of length $n = 2^m - 1$ and generator $g(x) = m_1(x)m_t(x)$ is at most five, and equality is possible (for example, if m is odd and $t = 13$). Here $m_i(x)$ denotes the minimum polynomial of α^i , for some primitive n th root of unity α . In [111], van Lint and Wilson show that if $g(x) = m_1(x)m_7(x)$ then the minimum distance is at most four, unless $m = 5$ and possibly $m \in \{11, 13, 17\}$. Their proof uses a deep theorem on the number of zeros of absolutely irreducible polynomials.

A combinatorial code $C(m, s)$ has length $n = \binom{m}{s}$ and its $\binom{m}{s} \times m$ generator matrix has all possible vectors of weight s as its columns. In [126], van Lint and Tolhuizen show that $C(m, s)$ has minimal weight $\binom{m-1}{s-1}$ for $s < m/2$, thus proving an earlier conjecture by Da Rocha.

Repeated-root cyclic codes are cyclic codes for which $\gcd(n, q) > 1$, where n is the length of the code and $GF(q)$ is the alphabet, which in turn ensures that the generator of the code has multiple zeros (repeated-roots). Answering a question of E.W. Gaal, van Lint argued in [130] that most such codes are not good. However, there are exceptions, for example, the even weight subcode of a shortened binary Hamming code; such codes are known to be optimal, and van Lint showed here that they are cyclic (after a suitable reordering of the coordinates). The methods of this paper are mostly of a combinatorial nature; for a more algebraic approach involving, for example, the Hasse derivative, see [CMSS91], where also other optimal repeated-root cyclic codes are described.

Combinatorial methods are used in [168] to show that a code of length n over an alphabet of size q with minimum distance 2 and *covering radius* 1 must have cardinality at least $q^{n-1}/(n-1)$. For $n = q = 4$ a direct construction is given of such a code with cardinality 28. We note that the previous record was 31 and that the afore-mentioned lower bound is value 22. (In 2005 P.R.J. Östergård a.o. (see [OQW05]) show that 28 is the minimum value.)

1.3. Other work related to applications

From 1986 on van Lint held a position of scientific consultant at Philips Research Laboratories, a position that was so dear to him that he even held on to it when he became dean of Eindhoven Technical University. From that time on he co-authored a number of papers motivated by practical applications. The earlier paper [48] with Pollak, published in 1975 but for the largest part conceived in 1965 during a stay at Bell Labs, can be seen as his first publication of that kind. This somewhat mysteriously titled paper is in fact concerned with optimal defense against a possible rocket attack by the enemy (which in those cold war times was of course uniquely determined). The defender is assumed to possess limited resources h to defend n properties (cities) C_1, \dots, C_n , where the value v_i of property C_i is known to both parties, against an

attacker that possesses total resources normalized to 1. A defensive strategy consist of dividing the total resources h among the entities; then, with full knowledge of the chosen defense the attacker distributes its offensive resources among the same cities. If the defense assigns resources h_i to city C_i and the attacker assigns a_i , then the attacker destroys the city (thereby gaining its value v_i) if and only if $a_i > h_i$. A strategy is called undominated if no other strategy exists that requires at most the same total resources and always performs at least as good whatever the values v_i and a_i . Interestingly, it turns out that for each n there exist only a finite number of undominated defensive strategies. As a consequence, for each value of h only the undominated defensive strategies that require total resources at most h need to be considered; the optimal strategy depends on the actual values v_i of the cities.

In [127] van Lint reviews some results on codes for channels with localized errors and variants, mostly providing new proofs or small improvements. For such channels, the sender (but not the receiver) knows the positions in which possible errors may occur, and may adapt the encoding accordingly. For example, the sender could provide some information about the possible locations of the errors in codeword headers. van Lint did not hold any patent himself, but he came close here since an informal talk by him at Philips Research later inspired Baggen and Tolhuizen to use similar ideas in coding for defective memories by recoding, see [TB99].

The papers [143,147] discuss strategies to minimize information leakage from secure processors. Some of the results also apply to information leakage in other cases, e.g., from the observed power consumption pattern of a smart card.

The much-cited paper [154] on codes with the identifiable parent property (IPP) concerns protection against software piracy. Multimedia publishers can “fingerprint” each copy of a distributed image with a unique watermark, a codeword which is invisibly embedded in the image. As a result, a customer that illegally redistributes his or her copy can be traced. This paper investigates collection of watermark codewords with the property that if a coalition of two customers create a new image by combining parts of their copies, then from this new image at least one of the perpetrators can still be identified. Mathematically, we consider a code C of length n over a q -ary alphabet Q (i.e., $C \subseteq Q^n$). For any two words $a, b \in C$, the set of descendants $D(a, b)$ of the pair $\{a, b\}$ is defined by $D(a, b) = \{x \in Q^n \mid x_i \in \{a_i, b_i\} \text{ for } i = 1, \dots, n\}$. If $c \in D(a, b)$ with $a, b \in C$ then we call $\{a, b\}$ a pair of parents for c and c a descendant of the code C . Now we say that the code C has the identifiable parent property (IPP) if for each descendant c of C at least one of the parents can be identified. That is, for each descendant c of C there exists a word $\pi(c) \in C$ such that each parent pair of c must contain $\pi(c)$. The paper investigates the largest size $F(n, q)$ of a q -ary code of length n that has IPP. In particular, it is shown that $c(q/4)^{n/3} \leq F(n, q) \leq 3q^{\lfloor n/3 \rfloor}$ for $n \geq 3$. Here the lower bound is obtained using Lovász local lemma, a probabilistic method, hence is non-constructive. A great many successor papers devoted to this problem and its generalizations have appeared; for some examples, see [AFS01,B103].

A (binary) sequence x_1, \dots, x_{L-1} is called (n, k) -universal if for each window $0 = w_1 < w_2 < \dots < w_k = m - 1$ of span m and size k , with $k \leq m \leq n$, each possible word from $\{0, 1\}^k$ occurs as $x_{i+w_1}, \dots, x_{i+w_k}$ for some i with $0 \leq i \leq L - m$. Universal sequences have applications in testing very large scale integration (VLSI) chips. The paper [146] investigates the minimal length $L(n, k)$ of (n, k) -universal sequences, and the minimal length $L^*(n, k)$ of the circular variant of such sequences. Note that de Bruijn sequences show that $L(k, k) = 2^k + k - 1$ and $L^*(n, k) = 2^k$. It is shown that $L(n, k) \leq n + c_k \log n$ for fixed $k \geq 3$, and it is conjectured that for each $k \geq 1$ there exists a number n_k such that $L^*(n, k) = n$ for $n \geq n_k$. It is known that $n_1 = 2$ and $n_2 = 5$; probably $n_3 = 19$, $n_4 = 67$, and $n_5 = 331$. As far as we know, this problem is still open.

2. The combinatorialist

2.1. Combinatorial problems

A very important aspect in Jack van Lint's mathematics was his interest in a wide variety of combinatorial problems. The source of these problems was either from industry, through his connections with Philips NatLab and with AT&T Bell Laboratories, or from his teaching experience in a variety of courses on combinatorics in Eindhoven and at Caltech, leading to his popular book written together with Rick Wilson, *A Course in Combinatorics*, that contains a delightful and broad selection of combinatorial techniques and results varying from extremal graph theory to finite geometry. A final source of many (mostly combinatorial, number theory, or analysis) problems was the Eindhoven problem solving group O.P. Lossers ('oplossers' is the Dutch word for (problem) solvers). Starting from 1968 he was for many years the inspiring force behind the team with a record number of published solutions in the problem section of the *American Mathematical Monthly*. Apart from the period of his rectorate of the university he was a faithful visitor of the biweekly meetings, where he invariably was the most active participant.

Among his favorite problems in combinatorics was the so-called van der Waerden conjecture, stating that the permanent of a doubly stochastic n by n matrix is at least $n!/n^n$ with equality occurring only if all entries are equal.

When he learned of the proof of this conjecture by Egoritsjev, published in a journal that was not easy accessible, he wrote down his own simplified version and so popularized this important result in his paper 'Notes on Egoritsjev's proof of the van der Waerden conjecture' [84,88,94].

A class of problems close to his heart are what he called $(0, 1, *)$ -problems. He was particularly enthusiastic about Peter Winkler's proof of the addressing problem for graphs, a proof that features in his survey paper ' $\{0, 1, *\}$ -distance problems in combinatorics.' From this paper we would like to state another problem concerning so-called tournament codes. The problem is still wide open and no improvements seem to have been made since the publication of his survey [106].

The problem consists of finding a set of $\{0, 1, *\}$ -vectors of length n (so in $\{0, 1, *\}^n$), such that for each pair at some coordinate position one has a zero, and the other a one, but not the other way round. An ingenious construction gives a set of size $n\sqrt{n}$ approximately, and there is an upper bound $n^{c \log n}$ due to Ron Graham, with a simple proof by Cor van Pul.

A completely different kind of research was his pioneering work with Jaap Seidel on equidistant point sets in elliptic geometry, motivated by the problem of determining the congruence order of the elliptic plane (or more generally elliptic n -space). In Euclidean terms we ask for sets of (concurrent) lines in \mathbf{R}^n , each pair having the same angle. The six main diagonals of the icosahedron are an example of six equidistant points in the elliptic plane. The relevance of this paper 'Equilateral point sets in elliptic geometry' [19] can hardly be overestimated. It reintroduced Seidel as a mathematical researcher after a 10 year period of administrative and organizational activities. It is one of the important starting points of parts of algebraic graph theory, containing the seeds of concepts like two-graphs and spherical codes and designs, and provided the natural geometrical model for the description of certain 2-transitive permutation representation, for example, Conway's simple group Co_3 or $\cdot 3$ is an automorphism group of an extremal set of 276 equiangular lines in \mathbf{R}^{23} .

2.2. Block designs

A block design with parameters $(v, k; b, r, \lambda)$ consists of a finite set P of v elements, called points, together with subsets B_1, \dots, B_b of P , each of size k , called blocks, with the property that each pair of points is contained in precisely λ blocks. In a block design furthermore each point is contained in precisely r blocks, where the parameters satisfy $bk = vr$ and $r(k - 1) = \lambda(v - 1)$. If the blocks are all distinct, then the design is called simple. However, nothing in the definition requires the blocks to be distinct, and in practical applications repetition of one or several of the blocks could even be advantageous. Nevertheless, the case of designs with repeated blocks was never systematically studied before the appearance of [32]. In this paper, van Lint and H.J. Ryser first give a new proof of Mann's inequality, stating that $e \leq b/v$ if a block is repeated e times; moreover, their methods allow them to conclude that equality is only possible if $e | \gcd(b, r, \lambda)$. They further show that the number t of distinct blocks satisfies $t \geq v$, with equality only if each block is repeated the same number of times, and also that $t \neq v + 1$. Finally, they construct many examples of block designs with repeated blocks, including several infinite families. This work is continued by van Lint in [36], where he investigates primitive repetition designs (PRD's), block designs with repeated blocks and $\gcd(b, r, \lambda) = 1$. Note that such designs cannot be obtained by simply duplicating all blocks from a simple design. The paper contains a list of all feasible parameter sets up to $v = 22$ and provides constructions for most of them. This work has recently been continued and extended in [DPS], where also some new bounds have been derived. For an alternative approach and for generalizations to Q -polynomial association schemes, see [Ho82, Ho84].

2.3. Other problems

In 1973 Deza showed that a collection of m binary words of length n and mutual distance $2k$, referred to here as an $(m, 2k, n)$ -code, is trivial if $m > k^2 + k + 2$. Here such a code is called trivial if the $m \times n$ matrix C that has the words of the code as rows has only columns with m or $m - 1$ equal entries. (Obviously, there are trivial codes with m as large as desired.) When van Lint heard from Deza about this problem he got very interested. First he showed in [38] that a non-trivial $(k^2 + k + 2, 2k, n)$ -code exists (for sufficiently large n) if and only if a $\text{PG}(2, k)$ exists. (Deza had already shown the "if" part of this theorem.) This of course left open the problem of determining the maximal m for which a non-trivial $(m, 2k, n)$ -code exists if no $\text{PG}(2, k)$ exists. The first interesting case is $k = 6$; here the above result gives $m \leq 43$. This was quickly brought down to 38, and an example was found showing that $m = 32$ is possible, but then progress got more difficult. van Lint handed out this problem to his master's students Janssen and Kolen as an assignment in completion of his famous course Discrete Math. I. After a long struggle they got the upper bound down to 34. There it stood for over one year, until finally J.I. Hall, who was visiting van Lint at that time, contributed the crucial idea that brought the upper bound down to 32, thus solving the problem. The common effort of the four contributors resulted in [64], which stands as a fine example of the ever stimulating role of van Lint towards his students.

A constant distance code pair is a pair (A, B) of binary codes, of the same length n , say, such that for some δ all words a, b with $a \in A$ and $b \in B$ have distance δ . In [109] van Lint and J.I. Hall showed that such a pair of codes consists of translates of orthogonal evenweight codes, thus proving that $|A||B| \leq 2^{2\lfloor n/2 \rfloor}$. They also determined when equality holds; it turns out that this occurs only for $\delta = n/2$ (if n is even) or $\delta \in \{(n - 1)/2, (n + 1)/2\}$ (if n is odd). The review paper [124] by van Lint contains among other things the generalization by van Pull [Pu87] stating that if, in addition, δ is prescribed, then $|A||B| \leq \max\{2^{2i} \binom{n-2i}{\delta-i} \mid 0 \leq i \leq \delta\}$,

with equality essentially only if $A = \{(\mathbf{x}, \mathbf{x}, \mathbf{0}) \mid \mathbf{x} \in \{0, 1\}^i\}$ and $B = \{(\mathbf{y}, \mathbf{1} + \mathbf{y}, \mathbf{z}) \mid \mathbf{y} \in \{0, 1\}^i, \mathbf{z} \in \{0, 1\}^{n-2i}, \text{weight}(\mathbf{z}) = \delta - i\}$.

3. The number theorist

The theory of modular forms was one of the first subjects in the mathematical research of Jack van Lint. At that time he was working at the University of Utrecht, and his thesis adviser was F. van der Blij. His PhD thesis [JvL1] was called Hecke Operators and Euler Products. Hecke operators act on the linear space of modular forms of a given weight and multiplier system for some group of finite index of the full modular group. These operators were first studied by Hecke, for modular forms of integral weight. van Lint gave a very general definition of Hecke operators, which acted on spaces of modular forms of non-integral weight, too. In particular he studied the effect of these operators on the Dedekind eta function, and the classical theta function, both modular forms of half integral weight. Of special interest with respect to Hecke operators are simultaneous eigenforms. Under certain conditions the Dirichlet series associated to these eigenforms have an Euler product representation. In his thesis van Lint gave a number of examples of such eigenforms, and he used his results to derive explicit formulae for the number of representations of a square as the sum of an odd number of squares.

As a follow-up four papers were published. We will discuss them briefly. Already in 1953 H.F. Sandham proved that if $r_k(m^2)$ is the number of representations of m^2 as a number of k squares, the Dirichlet series with the $r_k(m^2)$ as coefficients has a product representation for $k = 3, 5, 7$. For an odd integer $k > 7$ this no longer holds. This is caused by the fact that the genus of the quadratic form $x_1^2 + \dots + x_k^2$ consists of more than one class of quadratic forms for $k > 8$. In [1] van Lint proved that Sandham's results can be generalized to odd $k > 7$ if in the Dirichlet series one takes the sum over odd m only, and if $r_k(m^2)$ is replaced by the average representation number of m^2 by quadratic forms in the genus of $x_1^2 + \dots + x_k^2$.

In the theory of modular forms an important role is played by the Dedekind eta function. This is a modular form of weight $\frac{1}{2}$ for the full modular group, with some multiplier system. In 1931 this multiplier system was determined by H. Rademacher, using Dedekind sums. In [2] van Lint found the same formula in a different way. He gave a description of the characters of the modular group in terms of the matrix entries. And this enabled him to write down an explicit formula for the multiplier system.

In [3] a more general definition of theta functions than the one he used in his thesis, using this time an integral positive definite quadratic form and two translation vectors, was given. These functions are in general modular forms not for the modular group but for some subgroup of finite index. The aim of the paper was to find linear combinations of these theta functions that are modular forms for the full group. This puts restrictions on the translation vectors that can be used. And also necessary conditions for the existence of such linear combinations were given.

The last paper in this series [4] again answers a question about Hecke operators. K. Wohlfahrt had already proved that all Hecke operators could be built up out of special operators defined by him, unless there are linear relations between certain transforms of the modular forms. In that case so-called singular operators could be defined. In [JvL1] the question when such linear relations occur was answered for the full modular group, and for a special subgroup, the theta group. In [4] this problem was solved again for this theta group, but in a different way.

In 1959 van Lint moved to the Technical University of Eindhoven (which was called Technische Hogeschool Eindhoven at that time). Starting in 1963 another series of papers on number theory was written, but these papers were definitely different from the previous ones. In [12,15,

17,18,21,90] the asymptotic behavior of several number theoretic functions was discussed. Some of them, i.e. [12,15,17] were joint work with N.G. de Bruijn, while some of the others contained references to earlier results of de Bruijn. In [12] two functions $F(x)$ and $G(x)$ were considered. They were defined by the sum over all $n \leq x$ of $f(n, x)$ and $f(n, n)$, respectively, where $f(n, x)$ is the number of integers not exceeding x which are products of powers of prime factors of n . It was shown that $F(x) \sim G(x)$ as $x \rightarrow \infty$. The next paper in this series was [15]. Let λ be a non-negative multiplicative function defined on the positive integers. The largest prime divisor of an integer n is denoted by $P(n)$. The authors considered the function $\Lambda_a(x, y)$, defined as the sum of $\lambda(n)n^a$ over those $n \leq x$ satisfying $P(n) \leq y$, and where $a \geq 0$. Under certain restrictions on the function λ they found asymptotic formulas for $\Lambda_a(y^u, y)$. Euler's function φ has the well-known property that the sum of $\varphi(d)$ over all divisors d of an integer M equals M . In [17] de Bruijn and van Lint were interested in partial sums that are much smaller than M . They considered sums of $\varphi(d)$ over divisors d of M such that $d < M/f(M)$ for some function f . Under certain conditions on f they proved that this partial sum is $o(M)$ for $M \rightarrow \infty$. In [18] and [21] asymptotic formulas for the functions specified in the titles were given. In [90] the smallest, respectively greatest prime factor of an integer n were denoted by $p(n)$ and $P(n)$ and P. Erdős and van Lint dealt with the sum of $p(n)/P(n)$ over all $n \leq x$. Their first result was that this sum is $\pi(x)(1 + o(1))$ as $x \rightarrow \infty$ and in the second part of the paper this result was even refined. The sum mentioned in the title of [14] played an important role in applications of the sieve method of A. Selberg. The main result of this paper stated that this sum can be expressed as $d(u) \log y + O(1)$, for some function d , where $u = \log x / \log y$.

Two more papers must be mentioned in this section: [16] and [22]. It was already an old result by Dirichlet that any arithmetic progression $l + jk$ with coprime k and l contains infinitely many primes. Let $\pi(x, k, l)$ denote the number of primes p in this progression such that $p \leq x$. In [16] van Lint and H.E. Richert obtained sharp upper estimates for $\pi(x, k, l)$ and $\pi(x, k, l) - \pi(x - y, k, l)$, thus improving considerably on earlier results of Brun–Titchmarsh and Klimov.

The last paper in this section, i.e. [22], stands apart from the rest a bit. For any irrational number θ let a_0, \dots, a_n be the fractional parts of $l\theta$ for $l = 0, \dots, n$, arranged in ascending order. Define $d_\theta(n)$ as the maximum distance between a_i and a_{i-1} , $1 \leq i \leq n + 1$, where $a_{n+1} = 1$. R.L. Graham and van Lint determined in [22] $\sup_\theta \liminf_{n \rightarrow \infty} nd_\theta(n) = \frac{1}{2}(1 + \sqrt{2})$ and $\inf_\theta \limsup_{n \rightarrow \infty} nd_\theta(n) = 1 + \frac{2}{5}\sqrt{5}$, using the simple continued fraction expansion of the number θ .

4. The geometer

van Lint's belief in the importance of geometry and discrete mathematics is visible in his research, and dominated his invited talk [102] at the 1983 International Congress of Mathematicians. He began with general comments concerning strongly regular graphs and partial geometries. Then he stated a theorem of R.C. Bose [Bo63] that gives a numerical sufficient condition in order that a strongly regular graph whose parameters would allow it to be the point graph of a partial geometry does, indeed, arise from a partial geometry. He gave a brief outline of the proof, and mentioned extensions due to A. Neumeier and to A. Brouwer.

He then described several non-existence results for partial geometries with special parameters ($pg(4, 5, 2)$, $pg(6, 9, 4)$, and $pg(4, 7, 1)$), and discussed recently constructed sporadic examples ($pg(5, 7, 3)$, $pg(6, 6, 2)$ and $pg(5, 18, 2)$). After a brief discussion of generalized quadrangles, he carefully defined a family of new ones in terms of generalized hexagons [Ka80].

While [Co81] provided the first description of a $pg(8, 9, 4)$, [93] gave a simpler description of its dual. An infinite family of $pg(2^{2n-1}, 2^{2n-1}U, 2^{2n-2})$ was constructed in [DDT80] using quadrics over $GF(2)$; when $n = 2$ this is the aforementioned $pg(8, 9, 4)$.

This ICM talk showed van Lint's breadth of interest in a wide variety of geometric ideas. Others of his geometric papers are similarly broad.

An *oval* in a symmetric (v, k, λ) -design (a.k.a. "projective design") is defined in [75] to be a set O of points, no three on a block, such that either $\lambda|(k-1)$ and $|O| = (k + \lambda - 1)/\lambda$, or $\lambda|k$ and $|O| = (k + \lambda)/\lambda$. This notion generalizes that of an oval or hyperoval of a finite projective plane. The paper discusses the fact that O is in a standard sense extremal in each case, deduces properties resembling ones in planes, and then discusses cases with small λ . Finally, ovals are studied from a coding-theoretic point of view, including a more detailed study when $\lambda = 2$ (biplanes).

Ovals appeared in [103] in a different context: van Lint studied the projective plane $PG(2, 4)$ in an attempt to either construct or show the non-existence of a partial geometry $pg(5, 28, 2)$ that would be related to the McLaughlin $srg(275, 112, 30, 56)$ [McL69]. While he introduced a way to view this graph using the projective plane, this attempt was unsuccessful, and led him to conjecture that the desired partial geometry does not exist (this question still appears to be open).

van Lint was intrigued by the existence question for *quasi-residual designs* whose parameters made them possible residual designs of symmetric designs but were not, in fact, residual designs [70, 129, 105]. Rather strikingly, [129] constructed a quasi-residual $2-(28, 10, 45)$ design for which the Bruck–Ryser–Chowla theorem prevents the existence of any possible associated symmetric $2-(43, 15, 5)$ design. On the other hand, [70] earlier constructed two quasi-residual designs that are not residual, while [105] constructed infinite families of such designs.

At a 1981 finite geometry conference in Rome, W.M. Kantor showed van Lint an elementary description recently learned from R.D. Baker of generalizations of the remarkable non-linear, distance-invariant Preparata codes [Pr68]. This description made it easy to study these codes (e.g., to determine their isomorphisms and automorphisms [Ka83]). van Lint was very enthusiastic. Although his book [JvL11] was about to be sent to the publisher, he was able to insert these new ideas (pp. 101–102). Then he, Baker and R.M. Wilson extended the methodology to another important family of non-linear codes, the Goethals codes. In [96] these families of non-linear codes were all presented in a very elegant manner.

At the same time that Preparata codes were being generalized and their study simplified in [96], another famous family of non-linear codes, the Kerdock codes [Ke72], was also discovered to belong to a much broader context (affine planes and orthogonal geometries [Ka82]). [97] surveys and summarizes results from these two papers (compare [JvL15, Chapters 12, 16]).

5. The educator

5.1. Mathematical education

Not only was Jack van Lint a brilliant lecturer, but he was interested in mathematical education in many ways, too. From 1986 to 1994 he was a member of the Executive Committee of ICMI (International Commission on Mathematical Instruction), and from 1978 to 1988 he was editor of the International Journal of Mathematics Education in Science and Technology. As a representative of ICMI he visited several ICME conferences (International Congress on Mathematics Education, once every four years). At the conferences in 1976 (Karlsruhe), 1980 (Berkeley), 1984 (Adelaide) and 1992 (Québec) he was an invited speaker, too. At the conference

in Karlsruhe he gave a talk about his ideas on mathematics teaching at the university, both for students majoring in mathematics and mathematics as a service subject (see [63]). A final version of this paper became a chapter in *New Trends in Mathematics Teaching*, a UNESCO report prepared by ICMI [77]. It was translated into Spanish [78], French [79] and Japanese [81]. Other ideas about the teaching of more specific aspects of mathematics can be found in [100,107,118,138,139,140].

In [139] van Lint gave his definition of discrete mathematics, and listed a range of topics that should be covered in courses in discrete mathematics. But furthermore he gave strong recommendations on how discrete mathematics should be taught: “teachers should avoid at all times to give students the impression that discrete mathematics is a hodgepodge of subjects that have nothing in common.” He wrote a number of papers especially for high school teachers, too. See for instance [35,108,115,133,152]. It was his aim to present topics of mathematics, in particular discrete mathematics, in a popular way. In the last few years he was very worried about the standard of the mathematics education, both national and international. In [173] he gave his view on the central examination of mathematics in the Netherlands. This produced many positive reactions from high school teachers, but the policy makers were not amused, to put it mildly.

Together with Kristina Reiss from Germany and Gila Hanna from Canada he organized in 2003 a workshop in Oberwolfach about the role of discrete mathematics and proof in the high school curriculum. It was his idea that at the end of the week there would be a collection of ideas and materials that could be used by high school teachers. It turned out differently. He could not go there because just before the start of the workshop he became ill. But inspired by ideas from this meeting [177] was written. Many examples of topics from discrete mathematics that can be used in high school were given. It appeared in June 2004, three months before he died. It was his last contribution to mathematics education.

5.2. *The mathematics of the CD and other applications*

van Lint loved to talk and write about the importance of discrete mathematics, and in particular error-correcting codes, in applications. Reliable digital communication is based on techniques from coding theory. Cryptography has to be added to protect the information against eavesdroppers and hackers.

van Lint had many reasons to stress this importance: to show the outside world the relevance of mathematics in modern society, to show the mathematical world why discrete mathematics should be part of the curriculum, and to motivate students to study abstract algebra, number theory and combinatorics.

Amazingly enough, organizers of conferences and mathematical journals kept asking him over and over again to write about these things. He always complied because each time there was a different audience that he could reach. This started in 1982 with [91] in which he uses NASA’s Deep Space program to explain the principles of coding theory: the binary symmetric channel, the notion of redundancy, the first order Reed–Muller code, error-correction and Shannon’s theorem about the capacity of a channel. His story about the mathematics in the coding on the CD appeared in many different variations and in five different languages. In [114,115] he mentioned CD’s for the first time, introduced Reed–Solomon codes (using arithmetic modulo 31) and product codes and explained their relevance for this application. In [152,153,155,163,164,165,175] he still discussed error-correcting codes but also explained why (d, k) constrained sequences play a role in the recording. The ones (pits) on a CD have to be separated by at least d and by at most k zeros (lands). This is again explained in [171], which also discusses applications of de

Bruijn sequences for location problems under noisy read-out, and of two-dimensional variants of de Bruijn sequences for improving acoustics in concert halls.

In [133] he described *write-once memories* as a potential future application. One can burn a pit on such a device but not undo that. Still, you want to use this memory device a few times for storing data. He showed how the Fano plane can be used to write 4 times a number between 1 and 7 on a memory device with 7 memory positions. Note that $4 \times \log_2 7 \approx 11.23!$

In [132] he explained to a general audience how a combinatorial search method, called *stochastic cooling*, can be applied to the so-called football pool problem. Actually this is a covering problem related to the covering radius of error-correcting codes.

6. And some more

6.1. Cryptography

In 1982 already, van Lint stimulated young researchers around him to study cryptography. A study group at the CWI (Amsterdam), headed by David Chaum, is the result. In [95] he explained to the mathematical community in the Netherlands why public key cryptography is relevant for society and interesting for mathematicians. He introduced the notion of one-way functions and gave a description of the RSA system and the knapsack system. He then continued by telling that the knapsack cryptosystem has already been broken and uses that to make it clear that for a system to be secure it does not suffice that the underlying mathematical principle is computationally hard (NP-complete). In [98] he explained the same for the computer science community.

His only direct contribution to cryptography is [178], which appeared after his death. It is a paper on visual cryptography. In “classical” visual cryptography, based on the OR function, an image is split over n participants, who each get a transparency as share. When an authorized group of people superimpose their shares, the image is recovered, while other groups cannot recover even a single pixel. Typically, individual pixels in the image are subdivided in subpixels, and the superimposed image will recover the original pixel, but with a loss of contrast. For example, if at least one subpixel in the superimposed image is white (the subpixels of all contributing transparencies are white/transparent) the whole pixel has to be viewed as white, while it is declared black if all subpixels forming the pixel are black. (Note that the underlying function is the OR.) In [178], the authors studied visual threshold schemes, but now based on the XOR function, which can be physically realized by making use of the polarization of light. One of their constructions makes use of Reed–Solomon codes.

6.2. Other mathematical problems

van Lint also wrote a number of papers aiming simply at solving a mathematical problem (some of his “applied” papers could also be characterized as such). To mention a few, in [5] van Lint, together with van Albada and Laman, solves the following conjecture by C.J. Titus and J.L. Ullman: if $0 \leq \phi_1 < \dots < \phi_n < 2\pi$, $0 \leq \varphi_1 < \dots < \varphi_n < 2\pi$, and $\sum_{j=1}^n e^{i\phi_j} = \sum_{j=1}^n e^{i\varphi_j} = 0$, then $\sum_{j=1}^n e^{i(\phi_j - \varphi_j)} \neq 0$.

Together with K. Post, another member of O.P. Lossers, van Lint answered a question posed by N.G. de Bruijn by showing that if $\varphi_2, \varphi_3, \dots$ is a complete orthonormal sequence in Hilbert space and φ_1 is arbitrary, then there exists an orthonormal sequence ψ_1, ψ_2, \dots such that $\|\varphi_n - \psi_n\| = O(f(n))$ ($n \rightarrow \infty$) if and only if $\sum_{n=1}^{\infty} f(n)$ is divergent [6].

Finally, with Murray Klamkin, the prolific problem solver, van Lint solved a problem in renewal theory that generalized some problems encountered several times by them through their connection with problem sections of various journals [33].

7. Books by Jack van Lint

- [JvL1] J.H. van Lint, Hecke operators and Euler products, PhD thesis, Utrecht, Rijksuniversiteit Utrecht, 1957.
- [JvL2] J.H. van Lint, Coding Theory, Springer-Verlag, Berlin, 1973.
- [JvL3] M. Hall Jr., J.H. van Lint (Eds.), Combinatorics: Proceedings of the Advanced Study Institute on Combinatorics, held at Nijenrode Castle, 1974, Breukelen, The Netherlands, 8–20 July, 1974, Mathematisch Centrum Amsterdam, Amsterdam, 1974.
- [JvL4] J.H. van Lint, Combinatorial Theory Seminar Eindhoven University of Technology, Springer-Verlag, Berlin, 1974.
- [JvL5] Peter J. Cameron, J.H. van Lint, Graph Theory, Coding Theory and Block Designs, Cambridge Univ. Press, Cambridge, 1975.
- [JvL6] M. Hall, J.H. van Lint (Eds.), Combinatorics: Proceedings of the NATO Advanced Study Institute, held at Nijenrode Castle, Breukelen, The Netherlands, 8–20 July, 1974, Reidel, Dordrecht, 1975.
- [JvL7] J.H. van Lint (Ed.), Inleiding in de Coderingstheorie, Mathematisch Centrum Amsterdam, Amsterdam, 1976.
- [JvL8] Stan T.M. Ackermans, J.H. van Lint, Algebra en Analyse, Academic, Schoonhoven, 1976.
- [JvL9] Peter J. Cameron, J.H. van Lint, Teorija Grafov, Teorija Kodirovanija i Blok-Sxemy, Nauka, Glavnaja Redakcija Fiziko-Matematicheskoy Literatury, Moskva, 1980.
- [JvL10] Peter J. Cameron, J.H. van Lint, Graphs, Codes and Designs, Cambridge Univ. Press, Oxford, 1980.
- [JvL11] J.H. van Lint, Introduction to Coding Theory, first ed., Springer-Verlag, Berlin, 1982.
- [JvL12] J.H. van Lint, Gerard van der Geer, Introduction to Coding Theory and Algebraic Geometry, Birkhäuser, Basel, 1988.
- [JvL13] J.H. van Lint, Bianma Lilun Daoyin, S.I., s.n., 1988.
- [JvL14] J.H. van Lint, J.W. Nienhuys, Discrete Wiskunde, Academic, Schoonhoven, 1991.
- [JvL15] P.J. Cameron, J.H. van Lint, Designs, Graphs, Codes and Their Links, Cambridge, Cambridge Univ. Press, 1991.
- [JvL16] J.H. van Lint, R. Tijdeman (Eds.), Cryptography and Data Protection: Proceedings of a Symposium at the Royal Netherlands Academy of Arts and Sciences on 19th December, 1990, North-Holland, Amsterdam, 1992.
- [JvL17] J.H. van Lint, Introduction to Coding Theory, third rev. and expanded ed., Springer-Verlag, Berlin, 1999.
- [JvL18] J.H. van Lint, R.M. Wilson, A Course in Combinatorics, second ed., Cambridge Univ. Press, Cambridge, 2001.

Acknowledgments

The third author thanks Ludo Tolhuizen, Guido Janssen, and J.I. Hall for providing some valuable background information and for careful proofreading.

References

- [1] J.H. van Lint, Über einige Dirichletsche Reihen, Proc. Kon. Nederl. Acad. Wetensch. Ser. A Math. Sci. 61 (1958) 56–60.
- [2] J.H. van Lint, On the multiplier system of the Riemann–Dedekind function η , Proc. Kon. Nederl. Acad. Wetensch. Ser. A Math. Sci. 61 (1958) 522–527.
- [3] F. van der Blij, J.H. van Lint, On some special theta functions, Proc. Kon. Nederl. Acad. Wetensch. Ser. A Math. Sci. 60 (1958) 508–513.
- [4] J.H. van Lint, Linear relations for certain modular forms, Math. Nachr. 20 (1959) 123–126.
- [5] P.J. van Albada, G. Laman, J.H. van Lint, On the Hermitean product of ordered point sets on the unit circle, Michigan Math. J. 7 (1960) 245–250.
- [6] J.H. van Lint, K.A. Post, A problem in Hilbert space, Proc. Kon. Nederl. Acad. Wetensch. Ser. A Math. Sci. 63 (1960) 409–411.
- [7] J.H. van Lint, Another sorting problem (problem 60-08), SIAM Rev. 3 (1961) 336–337.
- [8] P.J. van Albada, J.H. van Lint, On a recurring process in arithmetic, Nieuw Arch. Wisk. 9 (1961) 65–73.
- [9] P.J. de Doelder, J.H. van Lint, Solution to problem 60-04, SIAM Rev. 3 (1961) 335–336.
- [10] J.H. van Lint, Über die Approximation von Zahlen durch Reihen mit positiven Gliedern, Colloq. Math. 9 (1962) 281–285.
- [11] P.J. van Albada, J.H. van Lint, Reciprocal bases for the integers, Amer. Math. Monthly 70 (1963) 170–174.
- [12] N.G. de Bruijn, J.H. van Lint, On the number of integers $\leq x$ whose prime factors divide n , Acta Arith. 8 (1963) 349–356.
- [13] N.G. de Bruijn, J.H. van Lint, On the asymptotic behaviour of some Dirichlet series with a complicated singularity, Nieuw Arch. Wisk. 11 (1963) 68–75.
- [14] J.H. van Lint, H.E. Richert, Über die Summe $\sum_{n \leq x, p(n) < y} \mu^2(n)/\varphi(n)$, Proc. Kon. Nederl. Acad. Wetensch. Ser. A Math. Sci. 67 (1964) 582–587.
- [15] N.G. de Bruijn, J.H. van Lint, Incomplete sums of multiplicative functions I, II, Proc. Kon. Nederl. Acad. Wetensch. Ser. A Math. Sci. 67 (1964) 339–359.
- [16] J.H. van Lint, H.E. Richert, On primes in arithmetic progressions, Acta Arith. 11 (1965) 209–216.
- [17] N.G. de Bruijn, J.H. van Lint, On partial sums of $\sum_{d|m} \varphi(d)$, Simon Stevin 39 (1965) 18–22.
- [18] P. Erdős, J.H. van Lint, On the number of positive integers $\leq x$ and free of prime factors $< y$, Simon Stevin 40 (1966) 73–76.
- [19] J.H. van Lint, J.J. Seidel, Equilateral point sets in elliptic geometry, Proc. Kon. Nederl. Acad. Wetensch. Ser. A Math. Sci. 69 (1966) 335–348.
- [20] H.J.L. Kamps, J.H. van Lint, The football pool problem for 5 matches, J. Combin. Theory 3 (1967) 315–325.
- [21] J.H. van Lint, Representation of 0 as $\sum_{k=-N}^N \epsilon_k k$, Proc. Amer. Math. Soc. 18 (1967) 182–184.
- [22] R.L. Graham, J.H. van Lint, On the distribution of $n\theta$ modulo 1, Canad. J. Math. 20 (1968) 1020–1024.
- [23] J.H. van Lint, Coding theory, in: J.H. van Lint, J.J. Seidel, P.C. Baayen (Eds.), Colloquium Discrete Wiskunde, in: MC Syllabus, vol. 5, Mathematisch Centrum, Amsterdam, 1968, pp. 51–75.
- [24] J.H. van Lint, Coding theory, Nieuw Arch. Wisk. 17 (1969) 128–132.
- [25] J.H. van Lint, On the nonexistence of perfect 2- and 3-Hamming-error-correcting codes over $GF(q)$, in: Program and abstracts of papers to be presented at the 1970 International Symposium on Information Theory, Noordwijk, The Netherlands, 15–19 June, 1970, IEEE, New York, 1970, pp. 3–4.
- [26] J.H. van Lint, On the nonexistence of perfect 2- and 3-Hamming-error-correcting codes over $GF(q)$, Inform. Control 16 (1970) 396–401.
- [27] J.H. van Lint, On the distribution of θ modulo 1, in: P. Turan (Ed.), Number Theory, in: Colloq. Math. Soc. János Bolyai, vol. 2, North-Holland, Amsterdam, 1970, pp. 139–140.
- [28] H.J.L. Kamps, J.H. van Lint, A covering problem, in: P. Erdős, A. Renyi, V.T. Sos (Eds.), Combinatorial Theory and its Applications, in: Colloq. Math. Soc. János Bolyai, vol. 4, North-Holland, Amsterdam, 1970, pp. 679–685.
- [29] J.H. van Lint, On the nonexistence of certain perfect codes, in: A.O.L. Atkin, B.J. Birch (Eds.), Computers in Number Theory: Proceedings of the Science Research Council Atlas Symposium, No. 2, held at Oxford, 18–23 August, 1969, Academic Press, London, 1971, pp. 277–282.
- [30] J.H. van Lint, Nonexistence theorems for perfect error-correcting codes, in: G. Birkhoff, M. Hall Jr. (Eds.), Computers in Algebra and Number Theory, in: SIAM–AMS Proceedings, vol. 4, Amer. Math. Soc., Providence, RI, 1971, pp. 89–95.
- [31] J.H. van Lint, Computer stamps from the Netherlands, J. Recreational Math. 1 (1971) 20–23.
- [32] J.H. van Lint, H. Ryser, Block designs with repeated blocks, Discrete Math. 3 (1972) 381–396.

- [33] M.S. Klamkin, J.H. van Lint, An asymptotic problem in renewal theory, *Statist. Neerlandica* 26 (Sonderheft) (1972) 191–196.
- [34] J.H. van Lint, A new description of the Nadler code, *IEEE Trans. Inform. Theory* 18 (1972) 825–826.
- [35] J.H. van Lint, De 13e internationale Wiskunde Olympiade, *Euclides: Maandblad voor de Didactiek van de Wiskunde* 48 (1972–1973) 47–58.
- [36] J.H. van Lint, Block designs with repeated blocks and $(b, r, \lambda) = 1$, *J. Combin. Theory Ser. A* 15 (1973) 288–309.
- [37] J.H. van Lint, Asymptotisch goede algebraïsche codes, *Verslagen van de Gewone Vergadering der Afd. Natuurkunde van de KNAW* 82 (1973) 171–173.
- [38] J.H. van Lint, A theorem of equidistant codes, *Discrete Math.* 6 (1973) 353–358.
- [39] E.R. Berlekamp, J.H. van Lint, J.J. Seidel, A strongly regular graph derived from the perfect ternary Golay code, in: J.N. Srivastava (Ed.), *A Survey of Combinatorial Theory*, North-Holland, Amsterdam, 1973, pp. 25–30.
- [40] J.H. van Lint, A determinant related to the Jacobi symbol, *Proc. Kon. Nederl. Acad. Wetensch. Ser. A Math. Sci.* 76 (1973) 189–191.
- [41] J.H. van Lint, Solution to problem 349, *Nieuw Arch. Wisk.* 22 (1974) 93–94.
- [42] J.H. van Lint, Solution to problem 350, *Nieuw Arch. Wisk.* 22 (1974) 94–111.
- [43] J.H. van Lint, Recent results on perfect codes and related topics, in: M. Hall, J.H. van Lint (Eds.), *Combinatorics, Part 1: Theory of Designs, Finite Geometry and Coding Theory*, Proceedings of the Advanced Institute on Combinatorics, held at Nijenrode Castle, Breukelen, The Netherlands, 8–20 July, 1974, in: *Mathematical Centre Tracts*, vol. 55, Mathematisch Centrum, Amsterdam, 1974, pp. 158–178.
- [44] J.H. van Lint, Equidistant point sets, in: T.P. McDonough, V.C. Mavron (Eds.), *Combinatorics, the Proceedings of the British Combinatorial Conference*, held in the University College of Wales, Aberystwyth, 2–6 July, 1973, in: *London Math. Soc. Lecture Note Ser.*, vol. 13, Cambridge Univ. Press, Cambridge, 1974, pp. 169–176.
- [45] B.L. Rothschild, J.H. van Lint, Characterizing finite subspaces, *J. Combin. Theory Ser. A* 16 (1974) 97–110.
- [46] P.J. Cameron, J.I. Hall, J.H. van Lint, T.A. Springer, H.C.A. van Tilborg, Translates of subgroups of the multiplicative group of a finite field, *Proc. Kon. Nederl. Acad. Wetensch. Ser. A Math. Sci.* 78 (1975) 285–289.
- [47] J.H. van Lint, Combinatorial designs constructed from or with coding theory, in: G. Longo (Ed.), *Information Theory, New Trends and Open Problems*, in: *CISM Courses and Lectures*, vol. 219, Springer-Verlag, Wien, 1975, pp. 227–262.
- [48] J.H. van Lint, H.O. Pollak, An asymmetric contest for properties of arbitrary value, *Philips Res. Rep.* 30 (1975) 40–55.
- [49] J.H. van Lint, A survey of perfect codes, *Rocky Mountain J. Math.* 5 (1975) 199–224.
- [50] J.H. van Lint, A problem of bipartite graphs, *Amer. Math. Monthly* 82 (1975) 55–56.
- [51] J.H. van Lint, H.J.L. Kamps, A comparison of a classical calculus test with a similar multiple choice test, *Educ. Stud. Math.* 6 (1975) 259–271.
- [52] J.H. van Lint, Recente ontwikkelingen in de combinatoriek, *Nieuw Arch. Wisk.* 24 (1976) 215–225.
- [53] J.H. van Lint, Perfecte codes, *Nieuw Tijdschrift voor Wiskunde* 63 (1976) 230–236.
- [54] L.M.H.E. Driessen, G.H.M. Frederix, J.H. van Lint, Linear codes supported by Steiner triple systems, *Ars Combin.* 1 (1976) 33–42.
- [55] J.H. van Lint, Voorbereidingen, in: J.H. van Lint (Ed.), *Inleiding in de Coderingstheorie*, in: *MC Syllabus*, vol. 31, Mathematisch Centrum, Amsterdam, 1976, pp. 1–9.
- [56] J.H. van Lint, De stelling van Shannon, in: J.H. van Lint (Ed.), *Inleiding in de Coderingstheorie*, in: *MC Syllabus*, vol. 31, Mathematisch Centrum, Amsterdam, 1976, pp. 10–18.
- [57] J.H. van Lint, Voorbeelden van codes, in: J.H. van Lint (Ed.), *Inleiding in de Coderingstheorie*, in: *MC Syllabus*, vol. 31, Mathematisch Centrum, Amsterdam, 1976, pp. 19–24.
- [58] J.H. van Lint, T.M.V. Janssen, Lineaire codes, in: J.H. van Lint (Ed.), *Inleiding in de Coderingstheorie*, in: *MC Syllabus*, vol. 31, Mathematisch Centrum, Amsterdam, 1976, pp. 25–37.
- [59] J.H. van Lint, P. van Emde Boas, Reed–Muller codes en de stelling van Chevalley, in: J.H. van Lint (Ed.), *Inleiding in de Coderingstheorie*, in: *MC Syllabus*, vol. 31, Mathematisch Centrum, Amsterdam, 1976, pp. 77–101.
- [60] J.H. van Lint, H.C.A. van Tilborg, Gelijkmatig verdeelde codes, in: J.H. van Lint (Ed.), *Inleiding in de Coderingstheorie*, in: *MC Syllabus*, vol. 31, Mathematisch Centrum, Amsterdam, 1976, pp. 102–117.
- [61] J.H. van Lint, Asymptotisch goede algebraïsche codes, in: J.H. van Lint (Ed.), *Inleiding in de Coderingstheorie*, in: *MC Syllabus*, vol. 31, Mathematisch Centrum, Amsterdam, 1976, pp. 128–135.
- [62] J.H. van Lint, Educacion matematica a nivel universitario, excluyendo la preparacion de profesores, *Boletin Informativo ICMI–CIAEM* 3 (1976) 31–39.
- [63] J.H. van Lint, Mathematics education at university level, in: *Proceedings of the 3rd International Congress on Mathematical Education, ICME-3*, Karlsruhe, 1976, pp. 174–184.

- [64] J.I. Hall, A.J.E.M. Jansen, A.W.J. Kolen, J.H. van Lint, Equidistant codes with distance 12, *Discrete Math.* 17 (1977) 71–83.
- [65] J.H. van Lint, Een oud probleem uit de computerindustrie, in: P. van Emde Boas, J.K. Lenstra, F. Oort, et al. (Eds.), *Een Pak Met een Korte Broek*, papers presented to H.W. Lenstra Jr. on the occasion of the publication of his “Euclidische getallenlichamen”, Amsterdam, s.n., 1977, pp. 1–3.
- [66] J.H. van Lint, Codes and designs, in: M. Aigner (Ed.), *Higher Combinatorics*, Proceedings of the NATO Advanced Study Institute, held in Berlin, West Germany, 1–10 September, 1976, in: NATO Adv. Study Inst. Ser. C, vol. 31, Reidel, Dordrecht, 1977, pp. 241–256.
- [67] J.H. van Lint, H.C.A. van Tilborg, J.R. Wiekema, Block designs with $v = 10$, $k = 5$, $\lambda = 4$, *J. Combin. Theory Ser. A* 23 (1977) 105–115.
- [68] D.M. Cvetkovic, J.H. van Lint, An elementary proof of Lloyd’s theorem, *Proc. Kon. Nederl. Acad. Wetensch. Ser. A Math. Sci.* 80 (1977) 6–10.
- [69] J.H. van Lint, Ovals et codages, *Cahiers du Centre d’Etudes de Recherche Operationelle* 20 (1978) 301–305.
- [70] J.H. van Lint, Non-embeddable quasi-residual designs, *Proc. Kon. Nederl. Acad. Wetensch. Ser. A Math. Sci.* 81 (1978) 269–275.
- [71] J.H. van Lint, Möbius vlakken, in: *Meetkunde, van Kunst tot Kunde, Vroeger en Nu, Vakantiecursus*, 1978, CWI, Amsterdam, 1978, pp. 57–65.
- [72] J.H. van Lint, F.J. MacWilliams, Generalized quadratic residue codes, *IEEE Trans. Inform. Theory* 24 (1978) 730–737.
- [73] C.W.H. Lam, J.H. van Lint, Directed graphs with unique paths of fixed length, *J. Combin. Theory Ser. B* 24 (1978) 331–337.
- [74] J.H. van Lint, Sphere-packings, codes, lattices and theta-functions, in: A. Schrijver (Ed.), *Packing and Covering in Combinatorics*, in: *Mathematical Centre Tracts*, vol. 106, Mathematisch Centrum, Amsterdam, 1979, pp. 141–160.
- [75] E.F. Assmus, J.H. van Lint, Ovals in projective designs, *J. Combin. Theory Ser. A* 27 (1979) 307–324.
- [76] J.H. van Lint, F.J. MacWilliams, N.J.A. Sloane, On pseudo-random arrays, *SIAM J. Appl. Math.* 36 (1979) 62–72.
- [77] J.H. van Lint, Mathematics education at university level, in: *New Trends in Mathematics Teaching*, prepared by the International Commission on Mathematical Instruction (ICMI), *The Teaching of Basic Sciences*, vol. 4, UNESCO, Paris, 1979, pp. 66–84.
- [78] J.H. van Lint, La educacion matematica al nivel universitario, in: *Nuevas Tendencias en la Enseñanza de la Matemática/preparado por la Comision Internacional de Educación Matemática*, UNESCO, Paris, 1979, pp. 71–91.
- [79] J.H. van Lint, L’enseignement des mathématiques à l’Université, in: *Tendances Nouvelles de l’Enseignement des Mathématiques*, prep. par la Commission Internationale de l’Enseignement Mathématique (CIEM), in: *Enseign. Sci. Math.*, vol. 4, UNESCO, Paris, 1979, pp. 70–89.
- [80] J.H. van Lint, Generalized quadratic-residue codes, in: G. Longo (Ed.), *Algebraic Coding Theory and Applications*, Summer School, 1978, Udine, in: *CISM Courses and Lectures*, vol. 258, Springer-Verlag, Berlin, 1979, pp. 285–310.
- [81] J.H. van Lint, *Diagaku oyobi gakuin ni okeru süga ku kyöiku*, Japanese translation of: *Mathematics Education at University Level*, 87–110.
- [82] A.A. Bruen, B.L. Rothschild, J.H. van Lint, On characterizing subspaces, *J. Combin. Theory Ser. A* 29 (1980) 257–260.
- [83] J.H. van Lint, Recente ontwikkelingen in de cryptografie, *Verslagen van de Gewone Vergadering der Afd. Natuurkunde van de KNAW* 89 (1980) 17–20.
- [84] J.H. van Lint, Notes on Egoritsjev’s proof of the van der Waerden conjecture, *Linear Algebra Appl.* 39 (1981) 1–8.
- [85] J.H. van Lint, A. Schrijver, Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields, *Combinatorica* 1 (1981) 63–73.
- [86] J.H. van Lint, Was heisst heute gut codieren?, in: 10. Österreichischer Mathematiker Kongress, Innsbruck, 1981.
- [87] F.R.K. Chung, E.N. Gilbert, R.L. Graham, J.B. Shearer, J.H. van Lint, Tiling rectangles with rectangles, *Math. Mag.* 55 (1982) 286–291.
- [88] J.H. van Lint, The van der Waerden conjecture, two proofs in one year, *Math. Intelligencer* 4 (1982) 72–77.
- [89] P.J. Cameron, J.H. van Lint, On the partial geometry $pg(6, 6, 2)$, *J. Combin. Theory Ser. A* 32 (1982) 252–255.
- [90] P. Erdős, J.H. van Lint, On the average ratio of the smallest and largest prime divisor of n , *Indag. Math.* 44 (1982) 127–132.
- [91] J.H. van Lint, *Mathematik und die Satellitenbilder der Planeten, Tetra*, *Zeitschrift für den Unterricht in Naturwissenschaften und Mathematik* 4 (1982) 39–41.
- [92] J.H. van Lint, Coding, decoding and combinatorics, in: R.J. Wilson (Ed.), *Applications of Combinatorics*, in: *Shiva Math. Ser.*, vol. 6, Shiva, Nantwich, 1982, pp. 67–74.

- [93] W.H. Haemers, J.H. van Lint, A partial geometry $pg(9, 8, 4)$, *Ann. Discrete Math.* 15 (1982) 205–212.
- [94] J.H. van Lint, The van der Waerden conjecture, *Ann. Discrete Math.* 18 (1983) 575–580.
- [95] J.H. van Lint, Public key cryptography, *Nieuw Arch. Wisk.* 1 (1983) 259–269.
- [96] R.D. Baker, J.H. van Lint, R.M. Wilson, On the Preparata and Goethals codes, *IEEE Trans. Inform. Theory* 29 (1983) 342–345.
- [97] J.H. van Lint, Kerdox codes and Preparata codes, *Congr. Numer.* 39 (1983) 25–41.
- [98] J.H. van Lint, Cryptografie, *Informatie, Maandblad voor Gegevensverwerking* 25 (1983) 47–51.
- [99] J.H. van Lint, Algebraic coding theory, in: M. Zweng, T. Green, J. Kilpatrick, et al. (Eds.), *Proceedings of the Fourth International Congress on Mathematical Education*, Birkhäuser, Boston, 1983, pp. 299–303.
- [100] J.H. van Lint, The influence of computers and informatics on mathematics and its teaching, *ICMI Discussion Document, l'Enseignement Mathématique* 30 (1984) 159–172.
- [101] A.E. Brouwer, J.H. van Lint, Strongly regular graphs and partial geometries, in: D.M. Jackson, S.A. Vanstone (Eds.), *Enumeration and Design*, Academic Press, London, 1984, pp. 85–122.
- [102] J.H. van Lint, Partial geometries, in: Z. Ciesielski, C. Olech (Eds.), *ICM, International Congress of Mathematicians: Proceedings, vol. 2*, Warszawa, Poland, 16–24 August, 1983, North-Holland, Amsterdam, 1984, pp. 1579–1589.
- [103] J.H. van Lint, On ovals in $PG(2, 4)$ and the McLaughlin graph, in: P.J. de Doelder, J. de Graaf, J.H. van Lint (Eds.), *Papers dedicated to J.J. Seidel*, Eindhoven University of Technology, EUT report. WSK, Dept. of Mathematics and Computing Science, 84-WSK-03, 1984, pp. 234–255.
- [104] J.H. van Lint, On equidistant binary codes of length $n = 4k + 1$ with distance $d = 2k$, *Combinatorica* 4 (1984) 321–323.
- [105] J.H. van Lint, V.D. Tonchev, Nonembeddable quasi-residual designs with large K , *J. Combin. Theory Ser. A* 37 (1984) 359–362.
- [106] J.H. van Lint, $\{0, 1, *\}$ distance problems in combinatorics, in: I. Anderson (Ed.), *Surveys in Combinatorics 1985, Invited Papers for the Tenth British Combinatorial Conference*, in: *London Math. Soc. Lecture Note Ser.*, vol. 103, Cambridge Univ. Press, Cambridge, 1985, pp. 113–135.
- [107] J.H. van Lint, The education of mathematical engineers, *Math. Ed. Apr.–Jun.* (1985) 11–14.
- [108] J.H. van Lint, On geometry and discrete mathematics, *De Nieuwe Wiskrant* 5 (1985) 45–47.
- [109] J.I. Hall, J.H. van Lint, Constant distance code pairs, *Proc. Kon. Nederl. Acad. Wetensch. Ser. A Math. Sci.* 88 (1985) 41–45.
- [110] J.H. van Lint, R.M. Wilson, On the minimum distance of cyclic codes, *IEEE Trans. Inform. Theory* 32 (1986) 23–40.
- [111] J.H. van Lint, R.M. Wilson, Binary cyclic codes generated by m_1m_7 , *IEEE Trans. Inform. Theory* 32 (1986) 283.
- [112] A.E. Brouwer, J.H. van Lint, Silno regularnie grafi i chastichnie geometrii, *Kibernet. Sb. (N.S.)* 24 (1987) 186–229.
- [113] J.H. van Lint, T.A. Springer, Generalized Reed–Solomon codes from algebraic-geometry, *IEEE Trans. Inform. Theory* 33 (1987) 305–309.
- [114] J.H. van Lint, Foutenverbetering op de compact disc, Voordracht gehouden op de 12de Gemeenschappelijke Studiedag NVvW-VVWL, Kapellen, 28 maart, 1987, *Wiskunde en Onderwijs* 13 (1987) 452–459.
- [115] J.H. van Lint, Foutenverbetering op de compact disc, *Euclides* 63 (1987/88) 97–101.
- [116] J.A. La Poutré, J.H. van Lint, An associative block design $ABD(10, 5)$ does not exist, *Util. Math.* 31 (1987) 219–225.
- [117] G.F.M. Beenker, J.H. van Lint, Optimal generalized Petersen graphs, *Philips J. Res.* 43 (1988) 129–136.
- [118] J.H. van Lint, Discrete mathematics, some personal thoughts, in: A.G. Howson, J.-P. Kahane, P. Lauginie, et al. (Eds.), *Mathematics as a Service Subject*, in: *ICMI Study Ser.*, Cambridge Univ. Press, Cambridge, 1988, pp. 58–62.
- [119] J.H. van Lint, Coding theory, in: J.H. van Lint, G. van der Geer (Eds.), *Introduction to Coding Theory and Algebraic Geometry*, in: *DMV-Seminar, vol. 12*, Birkhäuser, Basel, 1988, pp. 9–33.
- [120] J.H. van Lint, Coding theory. Introduction, *IEEE Trans. Inform. Theory* 34 (1988) 1274–1275.
- [121] J.H. van Lint, Chief guest's address at the annual conference of AIMT on 30th January, 1988, *Indian J. Math. Teaching* 14 (1988) 31–32.
- [122] J.H. van Lint, Recent results on covering problems, in: T. Mora (Ed.), *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proceedings of the 6th International Conference, AAEC-6, Rome, Italy, 4–8 July, 1988*, in: *Lecture Notes in Comput. Sci.*, vol. 357, Springer-Verlag, Berlin, 1989, pp. 7–21.
- [123] P.J.M. Laarhoven, J.H. van Lint, E.H.L. Aarts, L.T. Wille, New upper bounds for the football pool problem for 6, 7, and 8 matches, *J. Combin. Theory Ser. A* 52 (1989) 304–312.

- [124] J.H. van Lint, Distance theorems for code pairs, in: G.S. Bloom, R.L. Graham, J. Malkevitch (Eds.), *Combinatorial Mathematics, Proceedings of the Third International Conference*, in: *Ann. New York Acad. Sci.*, vol. 555, New York Academy of Sciences, New York, 1989, pp. 421–424.
- [125] J.H. van Lint, Algebraic geometry codes, in: E.W. Gaal, C.P.M.J. Baggen (Eds.), *Proceedings of the First Concern Contact Meeting on Error-Correcting Codes*, in: *Nat. Lab. Report*, vol. 6362, Philips Research Laboratories, Eindhoven, 1989, pp. 4–9.
- [126] L.M.G.M. Tolhuizen, J.H. van Lint, On the minimum distance of combinatorial codes, *IEEE Trans. Inform. Theory* 36 (1990) 922–923.
- [127] J.H. van Lint, Coding for channels with localized errors, in: W.H.J. Feijen, A.J.M. van Gasteren, D. Gries (Eds.), *Beauty is Our Business, a Birthday Salute to Edsger W. Dijkstra*, Springer-Verlag, Berlin, 1990, pp. 274–279.
- [128] J.H. van Lint, Algebraic geometric codes, in: D. Ray-Chaudhuri (Ed.), *Coding Theory and Design Theory, Part I: Coding Theory*, in: *IMA Vol. Math. Appl.*, vol. 20, Springer-Verlag, Berlin, 1990, pp. 137–162.
- [129] J.H. van Lint, V.D. Tonchev, I.N. Landgev, A new design, in: D. Ray-Chaudhuri (Ed.), *Coding Theory and Design Theory, Part II: Design Theory*, in: *IMA Vol. Math. Appl.*, vol. 21, Springer-Verlag, Berlin, 1990, pp. 251–256.
- [130] J.H. van Lint, Repeated-root cyclic codes, *IEEE Trans. Inform. Theory* 37 (1991) 343–345.
- [131] P.J.N. de Rooij, J.H. van Lint, More on the minimum distance of cyclic codes, *IEEE Trans. Inform. Theory* 37 (1991) 187–189.
- [132] J.H. van Lint, Stochastisch koelen en de voetbalpool, *Verslagen van de Gewone Vergadering der Afd. Natuurkunde van de KNAW* 101 (1992) 39–44.
- [133] J.H. van Lint, Recycling van ponskaarten?, *Euclides* 67 (1991–1992) 132–135.
- [134] M.J.M. van Eupen, J.H. van Lint, On the minimum distance of ternary cyclic codes, *IEEE Trans. Inform. Theory* 39 (1993) 409–422.
- [135] R.J.M. Vaessens, E.H.L. Aarts, J.H. van Lint, Genetic algorithms in coding theory—A table for $A_3(n, d)$, *Discrete Appl. Math.* 45 (1993) 71–87.
- [136] J.H. van Lint, Codes and combinatorial designs, in: D. Jungnickel, S.A. Vanstone (Eds.), *Coding Theory, Design Theory, Group Theory, Proceedings of the Marshall Hall Conference*, Wiley-Interscience, New York, 1993, pp. 31–39.
- [137] J.H. van Lint, V.D. Tonchev, A class of non-embeddable designs, *J. Combin. Theory Ser. A* 62 (1993) 252–260.
- [138] J.H. van Lint, A European view of a course on discrete mathematics, *New England Math. J.* 25 (1993) 18–19.
- [139] J.H. van Lint, What is discrete mathematics and how should we teach it?, in: *Proceedings of the 7th International Congress on Mathematical Education, ICME*, Presses de l'Univ. Laval, Sainte-Foy, 1994, pp. 367–368 (abstract).
- [140] J.H. van Lint, What is discrete mathematics and how should we teach it?, in: D.F. Robitaille, D.H. Wheeler, C. Kieran (Eds.), *Selected Lectures from the 7th International Congress on Mathematical Education*, Laval University, Québec, 17–23 August, 1992, Presses de l'Université Laval, Sainte-Foy, 1994, pp. 263–270.
- [141] J.H. van Lint, Preface, *Linear Algebra Appl.* 226/228 (1995) 1–8.
- [142] J.H. van Lint, Codes, in: R.L. Graham, M. Grötschel, L. Lovasz (Eds.), *Handbook of Combinatorics*, vol. 1, Elsevier, Amsterdam, 1995, pp. 773–807.
- [143] H.D.L. Hollmann, J.P.M.G. Linnartz, J.H. van Lint, C.P.M.J. Baggen, L.M.G.M. Tolhuizen, Protection of software algorithms executed on secure modules, in: P.H. Hartel, P. Paradinas, J.-J. Quisquater (Eds.), *Proceedings CARDIS 1996, Smart Card Research and Advanced Applications*, 2nd International Conference CARDIS 1996, CWI, Amsterdam, The Netherlands, 16–18 September, 1996, CWI, Amsterdam, 1996, pp. 133–143.
- [144] J.H. van Lint, Coding theory, *Images of SMC Research 1996*, Amsterdam, Stichting Mathematisch Centrum, 1996, pp. 113–121.
- [145] J.H. van Lint, Uit de verdediging!, *ITW Nieuws* 6 (1996) 2.
- [146] H.D.L. Hollmann, J.H. van Lint, Universal sequences, *Appl. Algebra Engrg. Comm. Comput.* 8 (1997) 347–352.
- [147] H.D.L. Hollmann, J.P.M.G. Linnartz, J.H. van Lint, C.P.M.J. Baggen, L.M.G.M. Tolhuizen, Protection of software algorithms executed on secure modules, *Future Gener. Comput. Syst.* 13 (1997) 55–63.
- [148] J.H. van Lint, Paul Erdős (Erdős Pál) 26 maart 1913–20 september 1996, levensbericht door J.H. van Lint, in: *Levensberichten en Herdenkingen 1998*, Koninklijke Nederlandse Akademie van Wetenschappen, Amsterdam, 1997, pp. 35–39.
- [149] T. Høholdt, J.H. van Lint, G.R. Pellikaan, Order functions and evaluation codes, in: T. Mora, H. Mattson (Eds.), *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proceedings of the 12th International Symposium, AAECC-12*, Toulouse, France, 23–27 June, 1997, in: *Lecture Notes in Comput. Sci.*, vol. 1255, Springer-Verlag, Berlin, 1997, pp. 138–150.
- [150] J.H. van Lint, On the number of blocks in a generalized Steiner system, *J. Combin. Theory Ser. A* 80 (1997) 353–355.

- [151] J.H. van Lint, Golay code, in: M. Hazewinkel (Ed.), *Encyclopedia of Mathematics*, Supplement I, Kluwer Academic, Dordrecht, 1997, p. 271.
- [152] J.H. van Lint, Wiskunde en de compact disc, *Nieuwe Wiskrant*, Tijdschrift voor Nederlands Wiskundeonderwijs 18 (1998) 12–16.
- [153] J.H. van Lint, Mathematics and the compact disc, Johan Bernoulli lecture, 1998, *Nieuw Arch. Wisk.* 16 (1998) 183–190.
- [154] H.D.L. Hollmann, J.H. van Lint, J.P.M.G. Linnartz, L.M.G.M. Tolhuizen, On codes with the identifiable parent property, *J. Combin. Theory Ser. A* 82 (1998) 121–133.
- [155] J.H. van Lint, The mathematics of the compact disc, *DMV-Mitteilungen* 4 (1998) 25–29.
- [156] J.H. van Lint, P. Erdős, Levensberichten en herdenkingen, *Mededelingen der Koninklijke Nederlandse Akademie van Wetenschappen*, 1998, pp. 35–39.
- [157] T. Høholdt, J.H. van Lint, G.R. Pellikaan, An elementary approach to algebraic geometry codes, *Congr. Numer.* 135 (1998) 25–35.
- [158] T. Høholdt, J.H. van Lint, G.R. Pellikaan, Algebraic geometry codes, in: V.S. Pless, W.C. Huffman (Eds.), *Handbook of Coding Theory*, vol. 2, Elsevier, Amsterdam, 1998, pp. 871–961.
- [159] J.H. van Lint, The Stan Ackermans Institute, *SEFI News* 76 (1999) 6.
- [160] J.H. van Lint, L.M.G.M. Tolhuizen, On perfect ternary constant weight codes, *Des. Codes Cryptogr.* 18 (1999) 231–234.
- [161] D. Jungnickel, J.H. van Lint, Guest editorial, *Des. Codes Cryptogr.* 17 (1999) 5–6.
- [162] D. Jungnickel, J.H. van Lint, Editorial, *Des. Codes Cryptogr.* 18 (1999) 5.
- [163] J.H. van Lint, Les mathématiques du disque compact, *Textes Conf. Math.* 4 (2000) 3–8.
- [164] J.H. van Lint, Kompaktskivans matematik, *Nordisk Matematisk Tidsskrift*, *Normat* 48 (2000) 115–122.
- [165] J.H. van Lint, Die Mathematik der Compact Disc, in: M. Aigner, E. Behrends (Eds.), *Alles Mathematik*, von Pythagoras zum CD-Player, Vieweg, Braunschweig, 2000, pp. 11–19.
- [166] J.H. van Lint, Coding theory and technology, lecture at La matemática como Base Conceptual de la Ciencia y la Tecnología, Simposio Internacional, Mathematics (the Conceptual Support of Science and Technology), Madrid, 11–12 Mayo, 2000.
- [167] T. Etzion, J.H. van Lint, On perfect constant weight codes, in: *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, vol. 56, 2001, pp. 131–134.
- [168] A. Blokhuis, S. Egner, H.D.L. Hollmann, J.H. van Lint, On codes with covering radius 1 and minimum distance 2, *Indag. Math. (N.S.)* 12 (2001) 449–452.
- [169] A. Blokhuis, J.H. van Lint, In memoriam Johan Jacob Seidel, *Nieuw Arch. Wisk.* 2 (2001) 207–209.
- [170] J.H. van Lint, Buitenlandse plaatsen, tegenwoordig heten ze zo, plezier en hoofdbreken dankzij quiz, *Filatelie* 79 (2001) 930–934.
- [171] J.H. van Lint, 0–1 Rijen, *Tijdschrift van het Nederlands Elektronica en Radiogenootschap* 66 (2001) 11–16.
- [172] J.H. van Lint, Rendement versus niveau, *Nieuw Arch. Wisk.* 3 (2002) 160–162.
- [173] J.H. van Lint, Reactie—Het eindexamen vwo B12, *Euclides* 78 (2002–2003) 20.
- [174] J.H. van Lint, Codes, correcteurs d’erreurs, commentaires, in: *Où en sont les mathématiques?*, Sous la Direct. de Jean-Michel Kantor, Vuibert, Paris, 2002, pp. 169–172.
- [175] J.H. van Lint, Wiskunde en de compact disc, in: *Tien Jaar NWD, een Lichtbundel.*, s.l., Freudenthal Instituut, 2004, pp. 34–39.
- [176] J.H. van Lint, Edsger Wybe Dijkstra, levensbericht door J.H. van Lint, in: *Levensberichten en Herdenkingen 2004*, Koninklijke Nederlandse Akademie van Wetenschappen, Amsterdam, 2004, pp. 32–36.
- [177] I. Anderson, A.G. van Asch, J.H. van Lint, Discrete mathematics in the high school curriculum, *Zentralblatt für Didaktik der Mathematik* 36 (2004) 105–116.
- [178] P. Tuyls, H.D.L. Hollmann, J.H. van Lint, L.M.G.M. Tolhuizen, XOR-based visual cryptography schemes, *Des. Codes Cryptogr.* 37 (2005) 169–186.

Other relevant references

- [AFS01] N. Alon, E. Fischer, M. Szegedy, Parent-identifying codes, *J. Combin. Theory Ser. A* 95 (2001) 349–359.
- [BI03] S.R. Blackburn, An upper bound on the size of a code with the k -identifiable parent property, *J. Combin. Theory Ser. A* 102 (2003) 179–185.
- [Bo63] R.C. Bose, Strongly regular graphs, partial geometries and partially balanced designs, *Pacific J. Math.* 13 (1963) 389–419.

- [CMSS91] G. Castagnoli, J.L. Massey, P.A. Schoeller, N. von Seeman, On repeated-root cyclic codes, *IEEE Trans. Inform. Theory* 37 (2) (March 1991).
- [Co81] A.M. Cohen, A new partial geometry with parameters $(s, t, \alpha) = (7, 8, 4)$, *J. Geom.* 16 (1981) 181–186.
- [DDT80] F. De Clerck, R.H. Dye, J.A. Thas, An infinite class of partial geometries associated with the hyperbolic quadric in $PG(4n - 1, 2)$, *European J. Combin.* 1 (1980) 323–326.
- [DPS] P. Dobcsányi, D.A. Preece, L.H. Soicher, On balanced incomplete block designs with repeated blocks, *European J. Combin.*, in press.
- [Ho82] H.D.L. Hollmann, Association schemes, Masters thesis, Eindhoven University of Technology, Dept. of Math. and Comp. Science, February 1982.
- [Ho84] H.D.L. Hollmann, t -Designs with repeated points in Q -polynomial association schemes, *Traitement du Signal* 1 (2) (1984) 163–168.
- [Ka80] W.M. Kantor, Generalized quadrangles associated with $G_2(q)$, *J. Combin. Theory Ser. A* 29 (1980) 212–219.
- [Ka82] W.M. Kantor, Spreads, translation planes and Kerdock sets, I, *SIAM J. Algebraic Discrete Methods* 3 (1982) 151–165;
W.M. Kantor, Spreads, translation planes and Kerdock sets, II, *SIAM J. Algebraic Discrete Methods* 3 (1982) 308–318.
- [Ka83] W.M. Kantor, On the inequivalence of generalized Preparata codes, *IEEE Trans. Inform. Theory* 29 (1983) 345–348.
- [Ke72] A.M. Kerdock, A class of low-rate nonlinear binary codes, *Inform. Control* 20 (1972) 182–187.
- [McE72] R.J. McEliece, Weight congruences for p -ary cyclic codes, *Discrete Math.* 3 (1972) 117–192.
- [McL69] J. McLaughlin, A simple group of order 898,128,000, in: *Theory of Finite Groups*, Benjamin, New York, 1969, pp. 109–111.
- [OQW05] P.R.J. Östergård, J. Quistorff, A. Wassermann, New results on codes with covering radius 1 and minimum distance 2, *Des. Codes Cryptogr.* 35 (2) (2005) 241–250.
- [Pr68] F.P. Preparata, A class of optimum non-linear double-error-correcting codes, *Inform. Contr.* 13 (1968) 378–400.
- [Pu87] C.L.M. van Pull, Some distance problems in coding theory, Doctoral thesis, Eindhoven University of Technology, 1987.
- [TB99] L.M.G.M. Tolhuizen, C.P.M.J. Baggen, Method and device for error protection of programmable memories, US patent 5,896,397, 13 April, 1999.
- [Ti73] A. Tietäväinen, On the non-existence of perfect codes over finite fields, *SIAM J. Appl. Math.* 24 (1973) 88–96.