

On the construction of optimal codes over \mathbb{F}_q

1

YUUKI KAGEYAMA

st301011@mi.s.osakafu-u.ac.jp

TATSUYA MARUTA

maruta@mi.s.osakafu-u.ac.jp

Department of Mathematics and Information Sciences

Osaka Prefecture University, Sakai, Osaka 599-8531, Japan

Abstract. In this paper we construct a q -divisible $[q^2 + q, 5, q^2 - q]_q$ code through projective geometry. As the projective dual of the code, we construct optimal codes, giving $n_q(5, d) = g_q(5, d) + 1$ for $q^4 - q^3 - q^2 + 1 \leq d \leq q^4 - q^3 - 2q$, $q \geq 3$, where $n_q(k, d)$ is the minimum length n for which an $[n, k, d]_q$ code exists and $g_q(k, d) = \sum_{i=0}^{k-1} \lceil d/q^i \rceil$. We also construct a $[g_q(k, d) + 1, k, d]_q$ code with $q \geq k \geq 5$ for $(k-2)q^{k-1} - (k-1)q^{k-2} - (q-k+1)q^{k-3} + 1 \leq d \leq (k-2)q^{k-1} - (k-1)q^{k-2}$.

1 Introduction

A linear code \mathcal{C} of length n , dimension k and minimum Hamming weight d over the field of q elements \mathbb{F}_q is referred to as an $[n, k, d]_q$ code. The weight distribution of \mathcal{C} is the list of numbers A_i which is the number of codewords of \mathcal{C} with weight i . We only consider linear codes having no coordinate which is identically zero. A fundamental problem in coding theory is to find $n_q(k, d)$, the minimum length n for which an $[n, k, d]_q$ code exists ([4]). A natural lower bound on $n_q(k, d)$ is the Griesmer bound: $n_q(k, d) \geq g_q(k, d) = \sum_{i=0}^{k-1} \lceil d/q^i \rceil$, where $\lceil x \rceil$ denotes the smallest integer $\geq x$. The values of $n_q(k, d)$ are determined for all d only for some small values of q and k , see [11]. In [12], it is proved that there exist no $[g_q(k, d), k, d]_q$ code for $q^{k-1} - q^{k-2} - q^2 + 1 \leq d \leq q^{k-1} - q^{k-2} - q$ for $k \geq 5$, $q \geq 3$. It is also known for $k \geq 5$, $q \geq 3$ that $[g_q(k, d) + 1, k, d]_q$ codes exist for $q^{k-1} - q^{k-2} - 2q + 1 \leq d \leq q^{k-1} - q^{k-2} - q$, but not known whether such codes exist or not for $q^{k-1} - q^{k-2} - q^2 + 1 \leq d \leq q^{k-1} - q^{k-2} - 2q$. We note that the part (ii) of Theorem 2.4 in [12] is stated wrongly. The statement should have been $n_q(k, d) \geq g_q(k, d) + 1$ for $s \geq 2$ because the existence of a $[g_q(k, d) + 1, k, d]_q$ code is unknown.

Problem 1. Does a $[g_q(k, d) + 1, k, d]_q$ code exist for $q^{k-1} - q^{k-2} - q^2 + 1 \leq d \leq q^{k-1} - q^{k-2} - 2q$ for $k \geq 5$, $q \geq 3$?

We give an answer for the case when $k = 5$ as follows:

¹This research is partially supported by Grant-in-Aid for Scientific Research of Japan Society for the Promotion of Science under Contract Number 24540138.

Theorem 1. *There exists a $[g_q(5, d) + 1, 5, d]_q$ code for $q^4 - q^3 - q^2 + 1 \leq d \leq q^4 - q^3 - 2q$.*

Corollary 2. $n_q(5, d) = g_q(5, d) + 1$ for $q^4 - q^3 - q^2 + 1 \leq d \leq q^4 - q^3 - 2q$.

We construct a q -divisible $[q^2 + q, 5, q^2 - q]_q$ code \mathcal{C} through projective geometry. As the projective dual of the code, we construct a q^2 -divisible $[q^4 + 1, 5, q^4 - q^3]_q$ code \mathcal{C}^* . And then, we construct $[g_q(k, d) + 1, k, d]_q$ codes for $q^4 - q^3 - q^2 + 1 \leq d \leq q^4 - q^3 - 2q$ by (geometric) puncturing.

It is known that $n_q(k, d) = g_q(k, d)$ for all $d \geq (k-2)q^{k-1} - (k-1)q^{k-2} + 1$ if $k \geq 3$ and that $n_q(k, d) = g_q(k, d) + 1$ for $(k-2)q^{k-1} - (k-1)q^{k-2} - q^2 + 1 \leq d \leq (k-2)q^{k-1} - (k-1)q^{k-2}$ if $q \geq 2k-3$ and $k \geq 6$, see [2]. We slightly improve this result. It can be proved applying Theorem 2 in [8] that there exists no $[g_q(k, d), k, d]_q$ code for $(k-2)q^{k-1} - (k-1)q^{k-2} - (k-2)q^{k-4} + 1 \leq d \leq (k-2)q^{k-1} - (k-1)q^{k-2}$ if $q \geq 2k-3$, $k \geq 4$. We show the existence of $[g_q(k, d) + 1, k, d]_q$ codes for such q, k and d .

Theorem 3. *There exists a $[g_q(k, d) + 1, k, d]_q$ code with $q \geq k \geq 5$ for $(k-2)q^{k-1} - (k-1)q^{k-2} - (q-k+1)q^{k-3} + 1 \leq d \leq (k-2)q^{k-1} - (k-1)q^{k-2}$.*

Corollary 4. $n_q(k, d) = g_q(k, d) + 1$ for $(k-2)q^{k-1} - (k-1)q^{k-2} - (k-2)q^{k-4} + 1 \leq d \leq (k-2)q^{k-1} - (k-1)q^{k-2}$ if $q \geq 2k-3$, $k \geq 4$.

It is known that $n_q(3, d) = g_q(3, d) + 1$ for $q^2 - 2q - \sqrt{2q} + 1 < d \leq q^2 - 2q$ with $q \geq 4$ and that $n_q(k, d) = g_q(k, d) + 1$ for $(k-2)q^{k-1} - (k-1)q^{k-2} - 2q + 1 \leq d \leq (k-2)q^{k-1} - (k-1)q^{k-2}$ for $q \geq 5$ when $k = 4$ and for $q \geq 11$ when $k = 5$, see [3] and [9]. See also Corollary 11 in Section 2 for $k = 4, 5$.

2 Construction

We denote by $\text{PG}(r, q)$ the projective geometry of dimension r over \mathbb{F}_q . A j -flat is a projective subspace of dimension j in $\text{PG}(r, q)$. The 0-flats, 1-flats, 2-flats, 3-flats and $(r-1)$ -flats are called *points*, *lines*, *planes*, *solids* and *hyperplanes* respectively. We denote by \mathcal{F}_j the set of j -flats of $\text{PG}(r, q)$ and by θ_j the number of points in a j -flat, i.e., $\theta_j = (q^{j+1} - 1)/(q - 1)$.

Let \mathcal{C} be an $[n, k, d]_q$ code having no coordinate which is identically zero. The columns of a generator matrix of \mathcal{C} can be considered as a multiset of n points in $\Sigma = \text{PG}(k-1, q)$ denoted by $\mathcal{M}_{\mathcal{C}}$. We see linear codes from this geometrical point of view. An i -point is a point of Σ which has multiplicity i in $\mathcal{M}_{\mathcal{C}}$. Denote by γ_0 the maximum multiplicity of a point from Σ in $\mathcal{M}_{\mathcal{C}}$ and let C_i be the set of i -points in Σ , $0 \leq i \leq \gamma_0$. We denote by $\Delta_1 + \cdots + \Delta_s$ the multiset consisting of the s sets $\Delta_1, \dots, \Delta_s$ in Σ . We write $s\Delta$ for $\Delta_1 + \cdots + \Delta_s$ when $\Delta_1 = \cdots = \Delta_s$. Then, $\mathcal{M}_{\mathcal{C}} = \sum_{i=1}^{\gamma_0} iC_i$. For any subset S of Σ , we

denote by $\mathcal{M}_{\mathcal{C}}(S)$ the multiset $\{P \in \mathcal{M}_{\mathcal{C}} \mid P \in S\}$. The *multiplicity of S with respect to \mathcal{C}* , denoted by $m_{\mathcal{C}}(S)$, is defined as the cardinality of $\mathcal{M}_{\mathcal{C}}(S)$, i.e., $m_{\mathcal{C}}(S) = \sum_{i=1}^{\gamma_0} i \cdot |S \cap C_i|$, where $|T|$ denotes the number of elements in a set T . Then we obtain the partition $\Sigma = \bigcup_{i=0}^{\gamma_0} C_i$ such that $n = m_{\mathcal{C}}(\Sigma)$ and $n-d = \max\{m_{\mathcal{C}}(\pi) \mid \pi \in \mathcal{F}_{k-2}\}$. Such a partition of Σ is called an $(n, n-d)$ -arc of Σ . Conversely an $(n, n-d)$ -arc of Σ gives an $[n, k, d]_q$ code in the natural manner. A line l with $t = m_{\mathcal{C}}(l)$ is called a t -line. A t -plane, a t -solid and so on are defined similarly. Denote by a_i the number of i -hyperplanes in Σ . The list of the values a_i is called the *spectrum* of \mathcal{C} , which can be calculated from the weight distribution by $a_i = A_{n-i}/(q-1)$ for $0 \leq i \leq n-d$. An $[n, k, d]_q$ code is called m -divisible if all codewords have weights divisible by an integer $m > 1$.

Lemma 5 ([14]). *Let \mathcal{C} be an m -divisible $[n, k, d]_q$ code with $q = p^h$, p prime, where $m = p^r$ for some $1 \leq r < h(k-2)$ satisfying $\lambda_0 > 0$. Then there exists a t -divisible $[n^*, k, d^*]_q$ code \mathcal{C}^* with $t = q^{k-2}/m$, $n^* = ntq - \frac{d}{m}\theta_{k-1}$, $d^* = ((n-d)q - n)t$.*

Note that a generator matrix for \mathcal{C}^* is given by considering $(n-d-jm)$ -hyperplanes as j -points in the dual space Σ^* of Σ for $0 \leq j \leq w-1$ [14]. \mathcal{C}^* is called the *projective dual* of \mathcal{C} , see also [1] and [5].

Lemma 6 ([13],[10]). *Let \mathcal{C} be an $[n, k, d]_q$ code and let $\bigcup_{i=0}^{\gamma_0} C_i$ be the partition of $\Sigma = \text{PG}(k-1, q)$ obtained from \mathcal{C} . If $\bigcup_{i \geq 1} C_i$ contains a t -flat Π and if $d > q^t$, then there exists an $[n - \theta_t, k, d']_q$ code \mathcal{C}' with $d' \geq d - q^t$.*

The code \mathcal{C}' in Lemma 6 can be constructed from \mathcal{C} by removing the t -flat Π from the multiset for \mathcal{C} . We denote the resulting multiset by $\mathcal{C} - \Pi$. In general, the method for constructing new codes from a given $[n, k, d]_q$ code by deleting the coordinates corresponding to some geometric object in $\text{PG}(k-1, q)$ is called *geometric puncturing*, see [10].

Recall that an $[n, k, d]_q$ code \mathcal{C} gives the partition $\bigcup_{i=0}^{\gamma_0} C_i$ of $\Sigma = \text{PG}(k-1, q)$ such that $n = m_{\mathcal{C}}(\Sigma)$ and $n-d = \max\{m_{\mathcal{C}}(\pi) \mid \pi \in \mathcal{F}_{k-2}\}$. Such a partition of Σ is called an $(n, n-d)$ -arc of Σ . Conversely an $(n, n-d)$ -arc of Σ gives an $[n, k, d]_q$ code in the natural manner. A set S of s points in $\text{PG}(r, q)$, $r \geq 2$, is called an s -arc if no $r+1$ points are on the same hyperplane, see [6] and [7] for arcs. When $q \geq r$, one can take a normal rational curve as a $(q+1)$ -arc in $\text{PG}(r, q)$ [[6], Theorem 27.5.1]. A set of m hyperplanes \mathcal{H} in Σ is called an m -arc of hyperplanes if the corresponding set of points forms an m -arc in the dual space Σ^* .

Let δ be a plane of $\Sigma = \text{PG}(4, q)$. Take a $(q+1)$ -arc $K = \{Q_0, Q_1, \dots, Q_q\}$ in δ and a line $\ell = \{P_0, P_1, \dots, P_q\}$ of Σ so that ℓ and δ have no common point. Let l_i be the line joining Q_i to P_i for $0 \leq i \leq q$. Setting $C_1 = (\bigcup_{i=0}^q l_i) \setminus \ell$ and $C_0 = \Sigma \setminus C_1$, we get a q -divisible $[q^2 + q, 5, q^2 - q]_q$ code \mathcal{C} .

Lemma 7. (1) *There exists a q -divisible $[q^2 + q, 5, q^2 - q]_q$ code \mathcal{C} with spectrum $(a_0, a_q, a_{2q}) = ((q^2 - q)/2, q^4 - q^2 + q + 1, (2q^3 + 3q^2 + q)/2)$.*

- (2) \mathcal{C}^* , the projective dual of \mathcal{C} , is a q^2 -divisible $[q^4 + 1, 5, q^4 - q^3]_q$ code. The multiset for \mathcal{C}^* contains $q - 1$ mutually disjoint lines.

Proof. (1) The spectrum of \mathcal{C} can be derived as follows. Let b_i be the number of lines in δ meeting K in exactly i points. Then we have $b_2 = (q^2 + q)/2$, $b_1 = q + 1$ and $b_0 = (q^2 - q)/2$. Let π be a solid in $\Sigma = \text{PG}(4, q)$. Assume π contains ℓ . Then π is a $2q$ -solid, a q -solid and a 0 -solid if π meets K in δ in a bisecant, a tangent and an external line, respectively. Assume π does not contain ℓ . If π contains none of l_0, l_1, \dots, l_q , then π is a q -solid. If π contains l_0 , then π contains none of l_1, \dots, l_q , so, π is a $2q$ -solid. Thus, $a_0 = b_0$, $a_{2q} = b_2 + q^2(q + 1)$, $a_q = \theta_4 - a_0 - a_{2q}$.

(2) It follows from Lemma 5 that \mathcal{C} is a q^2 -divisible $[q^4 + 1, 5, q^4 - q^3]_q$ code. Let ℓ^* and l_i^* be the planes in the dual space Σ^* of Σ corresponding to ℓ and l_i in Σ , respectively, for $0 \leq i \leq q$. Let $L_i = \ell^* \cap l_i^*$. Then, L_i is a 1-line in ℓ^* for \mathcal{C}^* and $\mathcal{L} = \{L_0, L_1, \dots, L_q\}$ forms a $(q + 1)$ -arc of lines in ℓ^* . Note that every 0-point in Σ^* for \mathcal{C}^* is a point on some plane l_i^* or a point in ℓ^* on some two lines from \mathcal{L} . Let R_0 be the 1-point in L_0 for \mathcal{C}^* . Since any line through R_0 meeting none of l_1^*, \dots, l_q^* and not being contained in $\ell^* \cup l_0^*$ contains no 1-point, the number of lines through R_i containing a 0-point is at most $(\theta_2 - \theta_1)q + 2q + 1 = q^3 + 2q + 1$. Hence, one can take at least $(\theta_3 - q^3 - 2q - 1)/q = q - 1$ mutually disjoint lines containing no 0-point for \mathcal{C}^* . \square

From Lemma 7 (2), we can construct a $[q^4 + 1 - t(q + 1), t, q^4 - q^3 - tq]_q$ code for $1 \leq t \leq q - 1$ from our code \mathcal{C}^* by geometric puncturing. This provides the codes needed in Theorem 1 when d is divisible by q . The rest of the codes required for the theorem can be obtained by puncturing these divisible codes.

Remark. The projective dual of a q^{k-3} -divisible $[q^{k-1} + 1, k, q^{k-1} - q^{k-2}]_q$ code is a q -divisible $[q^2 + q, k, q^2 - q]_q$ code for $k \geq 4$. For $k = 4$, one can construct q -divisible $[q^2 + q, 4, q^2 - q]_q$ code from q skew lines in $\text{PG}(3, q)$. But for $k \geq 6$, the existence of a q -divisible $[q^2 + q, k, q^2 - q]_q$ code is unknown except for the extended ternary Golay code ($k = 6$ and $q = 3$).

The following result is interpreted from the necessary and sufficient condition for the existence of Griesmer codes of Belov type, see [4], [5].

Theorem 8 ([4]). *For given positive integers s and $u_r \leq \dots \leq u_1 < k$ satisfying $u_i > u_{i+q-1}$ for $1 \leq i \leq r - q + 1$, there exists a $(u_j - 1)$ -flat Δ_{u_j-1} in $\Sigma = \text{PG}(k - 1, q)$ for $1 \leq j \leq r$ such that the multiset $s\Sigma$ contains the multiset $\Delta_{u_1-1} + \dots + \Delta_{u_r-1}$ if and only if $\sum_{i=1}^m u_i \leq sk$, where $m = \min\{s + 1, r\}$.*

Note that in the proof of Theorem 2.12 in [4], $A(f_1(x)), \dots, A(f_k(x))$ with $\deg f_i = 1$ for $1 \leq i \leq k$ correspond to k distinct hyperplanes whose defining vectors give a k -arc in $\text{PG}(k - 1, q)$.

For $k = 4$, it is known that $n_q(4, d) = g_q(4, d)$ for $d \geq 2q^3 - 3q^2 + 1$ for all q and that $n_q(4, d) = g_q(4, d) + 1$ for $2q^3 - 3q^2 - q + 1 \leq d \leq q^3 - 3q^2$ for $q \geq 4$.

Lemma 9. *There exists a $[g_q(4, d) + 1, 4, d]_q$ code for $2q^3 - 4q^2 + 1 \leq d \leq 2q^3 - 3q^2$ for any q .*

Proof. Let H_1, H_2, H_3 be three planes in $\Sigma = \text{PG}(3, q)$ such that $H_1 \cap H_2 \cap H_3$ is a point, say P . Then the multiset $\mathcal{S} = 2\Sigma + P - (H_1 + H_2 + H_3)$ gives a $[g_q(4, d) + 1, 4, d]_q$ code for $d = 2q^3 - 3q^2$ and the set of 0-points in the multiset \mathcal{S} consists of three lines through P . So, one can take $q - 1$ lines l_1, l_2, \dots, l_{q-1} containing none of the 0-points. Hence, by Lemma 6, the multiset $\mathcal{S} - (l_1 + \dots + l_t)$ gives a $[g_q(4, d) + 1, 4, d]_q$ code for $d = 2q^3 - 3q^2 - tq$ for $1 \leq t \leq q - 1$. The other codes required can be obtained by puncturing. \square

For $k = 5$, we can prove the following similarly.

Theorem 10. *There exists a $[g_q(5, d) + 1, 5, d]_q$ code for $3q^4 - 5q^3 + 1 \leq d \leq 3q^4 - 4q^3$ for any q .*

Corollary 11. $n_q(k, d) \leq g_q(k, d) + 1$ for any q for

- (a) $2q^3 - 4q^2 + 1 \leq d \leq 2q^3 - 3q^2$ when $k = 4$.
- (b) $3q^4 - 5q^3 + 1 \leq d \leq 3q^4 - 4q^3$ when $k = 5$.

Problem 2. Does a $[g_q(k, d) + 1, k, d]_q$ code exist for $(k - 2)q^{k-1} - kq^{k-2} + 1 \leq d \leq (k - 2)q^{k-1} - (k - 1)q^{k-2}$ for $k \geq 6$?

To prove Theorem 3, it suffices to show the following.

Lemma 12. *There exists a $[g_q(k, d) + 1, k, d]_q$ code with $q \geq k \geq 5$ for $d = (k - 2)q^{k-1} - (k - 1)q^{k-2} - \sum_{i=1}^{k-3} t_i q^i$ with $0 \leq t_{k-3} \leq q - k$ and $0 \leq t_j \leq q - 1$ for $1 \leq j \leq k - 4$.*

Proof. Let $\{H_1, H_2, \dots, H_k\}$ be a k -arc of hyperplanes in $\Sigma = \text{PG}(k - 1, q)$, that is, at most $k - 1$ hyperplanes of which are on a same point. Then, $H_1 \cap \dots \cap H_{k-1}$ is a point, say P , and $P \notin H_k$. Let \mathcal{S} be the multiset given by the $k - 2$ copies of Σ plus P with $k - 1$ hyperplanes H_1, \dots, H_{k-1} deleted, i.e., $\mathcal{S} = (k - 2)\Sigma + P - (H_1 + \dots + H_{k-1})$ and let \mathcal{C} be the code given by \mathcal{S} . Then \mathcal{C} is a $[g_q(k, d) + 1, k, d]_q$ code with $d = (k - 2)q^{k-1} - (k - 1)q^{k-2}$, and the set of 0-points in Σ consists of $k - 1$ lines through P meeting H_k in $k - 1$ points. Let $\pi_i = H_k \cap H_i$ for $1 \leq i \leq k - 1$. Then, the set $\{\pi_1, \dots, \pi_{k-1}\}$ forms a $(k - 1)$ -arc of $(k - 3)$ -flats in H_k and the multiset $\mathcal{M}_{\mathcal{C}}(H_k)$ can be written as $\mathcal{M}_{\mathcal{C}}(H_k) = (k - 2)H_k - (\pi_1 + \dots + \pi_{k-1})$. Since $(k - 1)$ -arcs in a $(k - 2)$ -flat are unique up to projective equivalence, it follows from Theorem 8 that the multiset $\mathcal{M}_{\mathcal{C}}(H_k)$ contains $\Delta_{u_1} + \dots + \Delta_{u_r}$, where Δ_{u_j} is a u_j -flat in H_k for $1 \leq j \leq r$ with $u_r \leq \dots \leq u_1 < k - 2$ such that at most $q - 1$ of u_1, \dots, u_r are the same value and that $\Delta_{u_j} = \pi_j$ for $1 \leq j \leq k - 1$. So, the multiset $\mathcal{M}_{\mathcal{C}}(H_k) - (\Delta_{u_1} + \dots + \Delta_{u_r})$ gives a $[g_q(k, d) + 1, k, d]_q$ code for $d = (k - 2)q^{k-1} - (k - 1)q^{k-2} - \sum_{i=1}^r q^{u_i}$. \square

References

- [1] A.E. Brouwer and M. van Eupen, The correspondence between projective codes and 2-weight codes, *Des. Codes Cryptogr.*, **11**, 261–266, 1997.
- [2] E.J. Cheon, A class of optimal linear codes of length one above the Griesmer bound, *Des. Codes Cryptogr.*, **51**, 9–20, 2009.
- [3] E.J. Cheon, T. Kato and S.J. Kim, Nonexistence of a $[g_q(5, d), 5, d]_q$ code for $3q^4 - 4q^3 - 2q + 1 \leq d \leq 3q^4 - 4q^3 - q$, *Discrete Math.*, **308**, 3082–3089, 2008.
- [4] R. Hill, Optimal linear codes, in: Mitchell C. (ed.) *Cryptography and Coding II*, pp. 75–104. Oxford Univ. Press, Oxford, 1992.
- [5] R. Hill and E. Koley, A survey of recent results on optimal linear codes, in: Holroyd F.C. et al (ed.) *Combinatorial Designs and their Applications*, pp.127–152, Chapman and Hall/CRC Press Research Notes in Mathematics. CRC Press. Boca Raton, 1999.
- [6] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Second edition, Clarendon Press, Oxford, 1998.
- [7] J.W.P. Hirschfeld and J.A. Thas, *General Galois Geometries*, Clarendon Press, Oxford, 1991.
- [8] A. Klein and K. Metsch, Parameters for which the Griesmer bound is not sharp, *Discrete Math.*, **307**, 2695–2703, 2007.
- [9] K. Kumegawa and T. Maruta, Nonexistence of some Griesmer codes of dimension 4 over \mathbb{F}_q , preprint.
- [10] T. Maruta, Construction of optimal linear codes by geometric puncturing, *Serdica J. Computing*, **7**, 73–80, 2013.
- [11] T. Maruta, Griesmer bound for linear codes over finite fields, <http://www.mi.s.osakafu-u.ac.jp/~maruta/griesmer.htm>.
- [12] T. Maruta, I.N. Landjev and A. Rousseva, On the minimum size of some minihypers and related linear codes, *Des. Codes Cryptogr.*, **34**, 5–15, 2005.
- [13] T. Maruta and Y. Oya, On optimal ternary linear codes of dimension 6, *Adv. Math. Commun.*, **5**, 505–520, 2011.
- [14] M. Takenaka, K. Okamoto and T. Maruta, On optimal non-projective ternary linear codes, *Discrete Math.*, **308**, 842–854, 2008.